TUTTI I SOFTWARE MIGLIORI SPIEGATI PASSO PASSO

HACKERS MAGAZINE.IT

ANDROID
Programmi messi a nudo

LIBRE OFFICE
Oracle Vs. Microsoft

WIRELESS
Quella del vicino è più veloce

HACKING
MULTIMEDIA
PROGRAMMING
COPY
NETWORKING
SYSTEM
WEB
P2P
SECURITY

HACKERS MAGAZINE N°65 - BIM. - ANNO 10 - 2011
€ 4.99 - DISTRIBUTORE: M-DIS DISTRIBUZIONE SPA
9 771720 767009 10066
WLF PUBLISHING

>SOMMARIO

TRA PASSATO E FUTURO

Si possono fare mille considerazioni su ciò che riteniamo ormai superato e quello che consideriamo il futuro. Nell'informatica, poi, questa condizione è banalmente espressa da un numero di versione oppure dall'inutilità di una tecnologia. Nessuno si sognerebbe di cercare metodi per leggere più velocemente delle schede perforate, così come nessuno si vanta di usare Windows 3.1.

A volte, però, le cose si sfumano e si può assistere a una nuova giovinezza di tecniche considerate più che superate. Non è un caso che ci rimettiamo a parlare di RAM disk. Tuttavia non si può passare il tempo recuperando vecchie tecnologie perché il futuro è già qui, nelle nostre case, nelle nostre mani. Allora dobbiamo cercare di capirlo, di smontarlo per ricostruirlo. Un po' come abbiamo fatto, grazie a qualche utility, con i file APK di Android. Con Google che ha sfasciato il delicato equilibrio tra Internet Explorer e Firefox e che, da oggi, ci ricorderà anche che possiamo installare delle App sul suo Chrome per renderlo migliore.

Faccende di ordinaria amministrazione per gente che deve adattarsi alle cose con la velocità del Web.

La redazione

HACKERSMAGAZINE.IT
Bimestrale - 4,99 euro

Sprea International
Via Torino, 51
Cernusco Sul Naviglio (MI) - Italy
Tel. (+39) 02.92.43.21
Fax (+39) 02.92.43.2.236

Direttore responsabile:
Luca Sprea - direttore@hackersmagazine.it

Redazione:
redazione@hackersmagazine.it

Stampa: Arti Grafiche Boccia S.p.a. - Salerno

Carta: Valpaco Paper Supply Chain Optimizer

Distribuzione:
M-Dis Distribuzione Spa
Via Cazzaniga, 19 – 20132 Milano

HACKERS MAGAZINE
Pubblicazione registrata al Tribunale di Milano il 15/07/2002 con il numero 414.

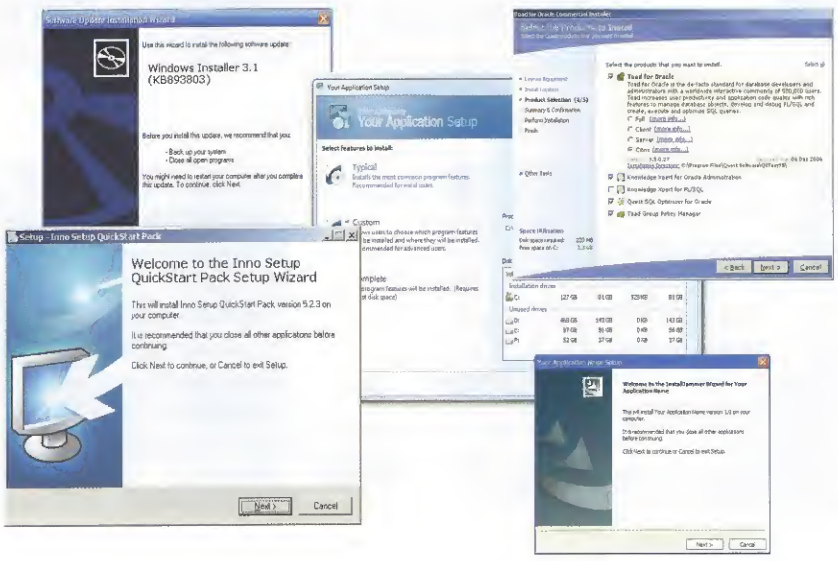
BASTA INSTALLER

PERCHÉ QUESTA VOGLIA DEI PRODUTTORI DI FARCI INSTALLARE QUALSIASI COSA RICORRENDO A PROGRAMMI SEMPRE PIÙ GRANDI, COMPLESSI E PESANTI? NON ESISTE UN INSTALLER STANDARD?

Nella storia dell'IT, l'idea di un programma che serve per installare altri programmi è abbastanza recente. Al debutto dei PC-IBM, bisnonni dei nostri moderni mostri di potenza, questo concetto era sconosciuto: i programmi giravano su floppy perché la maggior parte dei PC non aveva nemmeno un hard disk. Poi, l'hardware standard disponibile si è evoluto e così anche il software. Diversi programmatori hanno iniziato a distribuire dei piccoli batch insieme ai loro programmi. Cose fatte in casa, semplici programmi che creavano una directory e copiavano qualche file dal floppy all'hard disk.

Poi, con l'evoluzione dei sistemi operativi, Windows in particolare, le cose sono un po' sfuggite di mano. Attualmente gli installers hanno raggiunto dimensioni enciclopediche e danno lavoro a migliaia di persone che non fanno altro che preparare programmi di installazione di programmi fatti da altri. La smania di avere un installer che copi i file, gestisca la licenza, faccia gli update prima della copia, dia suggerimenti all'utente e migliaia di altre cose è talmente radicata che capitano utility che scaricate senza installer, magari in versione portable, passano sulla Rete leggere come piume mentre con il loro comodo programma di installazione risultano spesso più pesanti di una collezione di DivX d'annata.

Una soluzione, almeno inizialmente, c'era. Forse presa dal rimorso di aver distribuito un sistema operativo piuttosto complesso, per non dir peggio, Microsoft si è accorta, nel 1999, che la situazione stava diventando paradossale ed ha iniziato a usare un proprio standard, da allora in poi distribuito con tutti i suoi prodotti: l'MSI. La versione 1.0 fu presentata ufficialmente al mondo il 9 giugno 1999, con il lancio di Office 2000 e il sistema di installazione si è evoluto nel corso degli anni, sia come flessibilità di installazione che come potenzialità. Oggi siamo alla versione 5.0 usata da Windows 7 ma lo standard è seguito, in pratica, da Microsoft e da pochissime altre case. Tutti gli altri usano sistemi differenti perché Microsoft, bontà sua, aveva in mente di trattare Windows Installer come qualsiasi altro prodotto closed source. Buoni propositi fino ad un certo punto, quindi, e fallimento della relativa missione. In compenso, ogni installazione è un'avventura diversa e anche questa varietà ha i suoi lati divertenti. Forse.



GUIDA

I SOFTWARE CONTENUTI NEL CD-ROM SONO SUDDIVISI IN 10 AREE TEMATICHE. ALCUNI DI ESSI SONO COLLEGATI AI TUTORIAL PUBBLICATI SULLA RIVISTA NELLE PAGINE CONTRASSEGNATE DAL LOGO "NEL CD".

HACKING

- Brutus
- SniffPass
- SmartSniff
- Cain&Abel
- PDF Unlocker
- Attack Tool Kit
- AirCrack-NG

INTERNET

- GetMail
- Thunderbird
- Inbox2
- YouTube Clip Extractor
- Chrome

PROGRAMMING

- TortoiseSVN
- FileHamster
- Install Creator
- Visual Basic 2008 Express
- MyGeneration
- ddx
- dex2jar
- Baksmali
- Jasmin
- File Helper DLL

SECURITY

- Message Smuggler
- Androsa FileProtector
- Crypt4Free
- KeePass
- SafeHouse Explorer
- Spyware Terminator
- Defensio
- RunScanner
- Port Detective

AL CD

UTILITY

- Wiztoo Monitor
- ProgDVB
- Springboard
- Win SCP Portable
- Libre Office
- Libre Office SDK
- Libre Office Help ITA

P2P

- qBittorrent
- FrostWire
- BitTorrent
- Deluge
- iMule
- SoMud
- TurboWire
- eMule ScarAngel
- Lphant 5
- DeHinter

SYSTEM

- Rsync
- Process Hacker
- SUMo
- DesktopOK
- Glary Utilities
- System Ninja
- Xinorbis
- Dropbox
- HDClone Free Edition
- Dataram RAMDisk

NETWORKING

- Proxee Free
- VisualRoute Lite 2010
- UltraVNC
- NetWorx
- WeFi
- KiTTY
- Network Probe
- LAN Search Pro
- OpenVPN
- InSSIDer

COPIARE

- XMedia Recode
- FreeRIP
- BurnAware Free
- FinalBurner Free
- Cdrtfe
- Explore&Burn
- CDClick i-Studio
- DVDShrink
- Ashampoo Burning Studio

MULTIMEDIA

- Anaglyph Maker
- Warning Banner Creator
- Swiff Player
- Imagemap Applet Builder
- PictureClip
- Paint.NET
- AWicons Lite
- FFdshow
- VIP CD Ripper
- AIMP

MULTIMEDIA

DIGITALE E ANALOGICO

I CODEC AUDIO: COSA SONO, DOVE INTERVENGONO E A COSA SERVONO.

di Little Rose
redazione@hakerjournal.it

Parliamo di codec audio ma potremmo parlare anche di codec video: il nostro computer, in un certo senso, prende in giro i nostri sensi facendoci percepire qualcosa di ricostruito come se fosse reale e affidandosi alle capacità del nostro cervello per simulare la realtà.

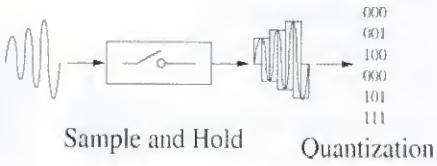
Ci sono molti fattori che influiscono sulla qualità del suono: la fedeltà all'originale reale dipende sia dal formato (il modo in cui il suono viene memorizzato), sia dal metodo di registrazione. Tra i due, il metodo di registrazione è quello che oggi crea i maggiori problemi, persino in un'epoca di file MP3. Caratteristica degli MP3, infatti, è la rimozione delle frequenze audio che non sono normalmente percepibili dagli esseri umani. Questo porta a una riduzione della quantità di dati e, di conseguenza, di un minor spazio occupato da ogni registrazione. Restando su livelli di compressione MP3 che mantengono alta la qualità, però, le differenze tra un file Wav uncompressed e un MP3 compresso con criterio sono minime, spesso indistinguibili anche da un orecchio ben allenato.

CATTIVO REGISTRATORE!

Per principio, la registrazione analogica acquisisce il segnale originale, proveniente magari da un'orchestra, con la più alta fedeltà possibile. Il suono viene acquisito così com'è, senza alcuna trasformazione. Il problema nasce, tuttavia, quando si può facilmente costatare che questo suono non è così puro come dovrebbe essere: i componenti elettronici, la perdita di segnale e i disturbi elettrici interferiscono facilmente con questo processo, provocando distorsioni, perdite di qualità e vere e proprie interruzioni di segnale. L'ideale sarebbe registrare in ambienti privi di ogni interferenza ma si tratta di una situazione impossibile: gli stessi componenti usati per registrare in modo analogico provocano interferenze tra loro e anche le apparecchiature di più alta qualità soffrono di problemi di perdita di segnale. I segnali digitali sono, invece, immuni a questi effetti, rendendo l'acquisizione in digitale una garanzia di ottenere i migliori risultati malgrado le approssimazioni a cui si è costretti per la registrazione dell'audio.

Il procedimento per cui un suono analogico diventa digitale si divide in diverse fasi: sampling, conversione (ADC), processo (DSP), riconversione (DAC), filtering.

Nel sampling si prende un segnale che varia col tempo e lo si spezza in tante sezioni all'interno delle quali questo segnale, voltaggio, risulta costante. Il numero di sezioni al secondo, misurato in hertz, è l'approssimazione a cui il suono viene registrato e ci pone immediatamente davanti alla limitazione più grande del suono digitale: al di sotto di una certa soglia,



La parte encoding dei codec trasforma un segnale continuo analogico in un segnale approssimato digitale. Un'operazione piuttosto delicata.

generalmente di 22050 Hz, il suono risulta palesemente povero e approssimato. Al di sopra, dai 44100 Hz in poi, nemmeno l'orecchio più fine può distinguere le differenze con la realtà. Un po' quello che avviene con i colori: se con immagini a 16 bit (65536 colori) si ingannano la maggior parte delle persone, con immagini a 32 bit (16 miliardi e oltre di colori) è solo la definizione, intesa come numero di punti che compongono l'immagine, che può svelare di non avere a che fare con la realtà.

Per tornare all'audio occorre segnalare che, teoricamente, il segnale audio in input che vogliamo registrare deve avere delle limitazioni: la sua frequenza più alta deve essere la metà dell'inverso del periodo di sampling (chiamata frequenza Nyquist). Se il sample contiene una o più frequenze sotto il Nyquist, bisogna prefiltrarlo per evitare una distorsione comunemente chiamata audio alialing.

DA ANALOGICO A DIGITALE

Dopo la preparazione del segnale tramite il sampling, ogni valore costante di voltaggio trovato viene digitalizzato dal processore ADC: Analog to Digital Converter. Generalmente, nella registrazione digitale in presa diretta, il lavoro è svolto da un componente dedicato che trasforma i livelli registrati in rappresentazioni binarie mentre sui computer di fascia bassa questo compito è lasciato alla CPU, con risultati scarsi per la perdita che avviene quando la CPU è sovraccarica a causa di altri processi in corso. La qualità della conversione dipende, ovviamente, dal numero di livelli possibili raggiungibili da questa sequenza di valori e si ottiene elevando 2 al numero di bit desiderati per la definizione del suono (chiamati anche bit di quantizzazione). Le conversioni più comuni utilizzano scale da 16 bit ma le attrezzature migliori arrivano a 24 e oltre: maggiore sarà il valore e più ampia sarà la scala di frequenze quantizzabili. Non è comunque necessario esagerare: frequenze troppo basse o troppo alte sono strutturalmente impossibili da udire per l'orecchio umano.

Qualsiasi lettore Mp3 deve includere una sezione di decodifica del segnale e diverse sezioni di filtro per trasformare una sequenza di bit compressi in un suono che è più o meno simile a quello reale.

A incaricarsi della conversione sui nostri computer è il codec: la prima parte del suo nome, infatti, prende il nome direttamente dalla C di ADC ed è in base al codec scelto che i criteri di selezione di frequenza e campionamento vengono scelti più o meno in automatico.

Il nostro segnale audio, ora, è già una sequenza di numeri raw che può essere salvata oppure trattata matematicamente per ottenere qualsiasi effetto desiderato. Quest'ultimo compito viene affidato solitamente a un processore DSP (Digital Signal Processor), decisamente più potente dell'ADC, che può svolgere i compiti più svariati: in studio di registrazione è il DSP che permette l'applicazione in tempo reale di effetti echo ma ad esso vengono anche demandati i compiti legati alla pulizia del segnale. A tal proposito occorre segnalare che i sintetizzatori digitali sono sostanzialmente dei DSP che generano sequenze di numeri non casuali secondo determinati comportamenti che vengono poi rielaborati da processori DSP.

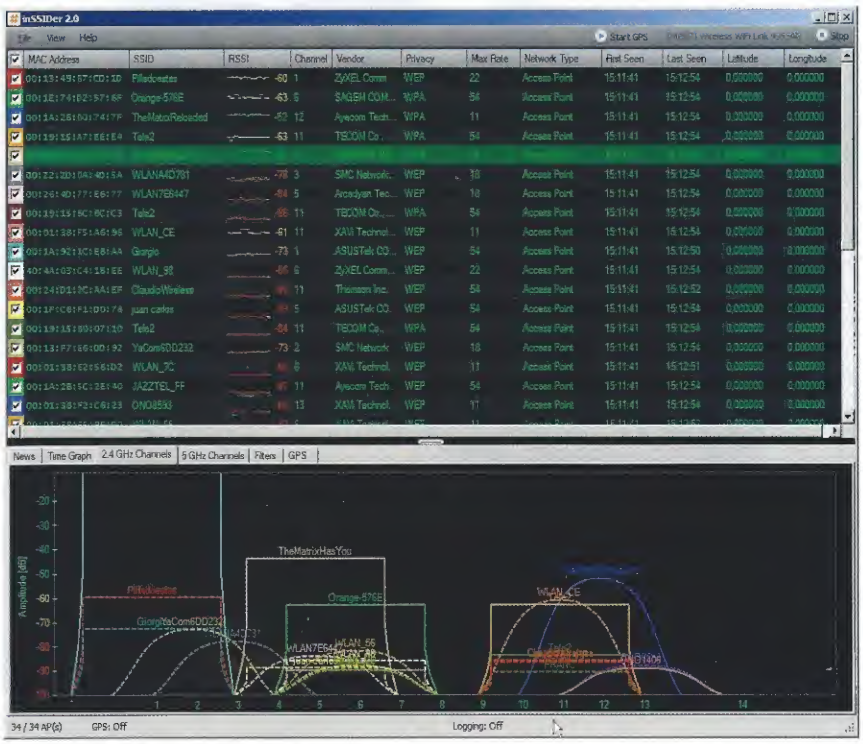
Prima di arrivare alle nostre orecchie, le registrazioni audio digitali subiscono una serie di processi estremamente vari che includono filtri hardware e software. Tutto per ingannarci.

PROCESSO INVERSO

La prima cosa che deve essere fatta per ascoltare il segnale digitale è quella di ritrasformarlo in segnale analogico. L'incaricato di questo processo è solitamente un processore DAC (Digital to Analog Converter) oppure un software in grado di emularlo parzialmente sulla CPU. L'emulazione è solo parziale in quanto il processo è strettamente fisico: il DAC deve leggere una sequenza di numeri e trasformarla in una corrente variabile alla frequenza corretta e al samplig giusto e questo avviene agendo comunque e sempre su componenti elettronici. La qualità, in questa fase, può subire degradi notevoli: le capacità del DAC non sono illimitate e così pure la sua velocità. Può capitare che un ADC di alta capacità crei file impossibili da riprodurre con alcuni DAC e sia necessario far intervenire, prima, un DSP software o hardware capace di ridurre la complessità dell'audio da riprodurre. Per evitare questi problemi, generalmente, a ogni ADC viene fatto corrispondere un DAC e, da qui, la sigla codec: visto come un unico componente, si tratta di due processi nettamente separati ma decisamente interdipendenti per la registrazione e la riproduzione del suono. L'ultimo passo fatto dal suono prima di arrivare alle nostre orecchie è il filtering: consiste nel prendere i voltaggi decodificati dal DAC, visti come tante scalette, e renderli più soft, con passaggi meno bruschi dall'uno all'altro, cercando di ricostruire la continuità persa con la digitalizzazione. Viene svolto da un filtro per le bande basse che elimina ogni frequenza ottenuta sopra quella Nyquist. L'effetto è quello di rendere più soft gli sbalzi di frequenza, aumentando l'inganno per l'orecchio e rendendo continuo un suono che è tutt'altro. Ovviamente, il livello di intervento del filtering può essere variato ma nelle apprecchiature professionali è limitato alle frequenze Nyquist: diversamente l'ascoltatore si renderà conto dell'inganno.

HACKING NEL CD

SEGNALI DAL VICINO



COME POSIZIONARE IL ROUTER WI-FI? COSA DISTURBA LA NOSTRA RETE? BASTA UN PROGRAMMA PER RISOLVERE I NOSTRI PROBLEMI.

di N4Break
redazione@hackerjournal.it

Inizialmente, i router wireless disponevano di una singola antenna e funzionavano a velocità decisamente basse, con scarsa copertura. L'evoluzione tecnologica ha moltiplicato le antenne, le capacità di compressione dei dati, le velocità di trasferimento e ha amplificato la copertura, permettendoci di coprire facilmente ampie aree usando un solo punto di accesso. Questo, però, non significa certo la fine dei problemi, anzi: in alcuni casi è solo l'inizio perché la facilità con cui diffondiamo il nostro segnale è pari a quella dei nostri vicini e in alcuni contesti, specialmente cittadini, l'affollamento di reti di terzi può interferire con la nostra Wi-Fi privata. La pubblicità, poi, ci ha convinto che il nostro router coprirà ampiamente qualsiasi area, anche se nella pratica vediamo quotidianamente che basta un muro di carta per vedere le prestazioni cadere in picchiata.

Quello che solo gli esperti dicono è che le onde del segnale si diffondono seguendo regole che non impediscono che si creino coni d'ombra e che anche i dispositivi più moderni e più veloci possono solo arginare il problema ma non risolverlo. Gli unici che possono fare qualcosa per diffondere al meglio il segnale dal nostro punto di accesso Wi-Fi siamo noi, posizionandolo al meglio, orientando le sue antenne e ricorrendo, quando necessario, a dispositivi aggiuntivi per ripetere il segnale (repeater) oppure usando antenne potenziate.

Un wardriving globale? No: inSSIDer esporta la posizione delle Wi-Fi per ritrovarle facilmente quando necessario.

In alto l'elenco delle reti trovate e tutti i dettagli tecnici relativi. In basso lo schema con le potenze di trasmissione e le sovrapposizioni di canali.

L'andamento delle reti nel tempo ci permette di rilevare i cambiamenti di segnale dovuti al posizionamento migliore del router.

ANALIZZARE POTENZA E FREQUENZA

Tra tutti i rimedi, il posizionamento corretto è quello che ha il minor costo, ovviamente, a fronte di benefici immediati ma è anche quello che risulta più complesso da operare perché richiede la misura della potenza del segnale: un argomento che la maggior parte degli utenti lasciano volentieri a tecnici esperti, spesso antennisti.

In realtà la questione è banale: spostando anche di poco un router, quanto segnale è possibile evitare di sprecare? Si possono creare riflessi del segnale che arrivino in ogni area che vogliamo coprire?

Tra le molte utility che ci semplificano questo compito, la più famosa è senz'altro NetStumbler: viene spesso usato nel wardriving ed è stato forse il primo strumento del genere alla portata della maggior parte degli utenti. Ultimamente, però, NetStumbler sta perdendo un po' di colpi, non tanto per le sue caratteristiche, sempre all'avanguardia, oppure per problemi di compatibilità con device wireless ma per l'assoluta mancanza di una versione funzionante su sistemi Windows 7 a 64 bit. Questo limita notevolmente l'applicazione di NetStumbler a contesti professionali, dove l'hardware subisce ricambi regolari.

Uno strumento meno conosciuto ma che si sta affermando in sua sostituzione è inSSIDer: open source, di aspetto professionale e semplice da usare. Da un punto di vista tecnico, isSSIDer non usa i driver della scheda wireless ma le API native disponibili sulla scheda stessa, bypassando Windows e permettendoci di ottenere risultati anche in condizioni svantaggiose. Inoltre non recupera solo l'elenco delle reti wireless disponibili ma ci permette, se collegato a un GPS, di geotaggarle e di recuperare anche una serie di altre informazioni: indirizzo MAC dell'access point che emette il segnale, la sua potenza, la chiave di codifica usata e via dicendo. Ogni rete individuata viene inserita in un database, facilmente consultabile e l'elenco può persino essere esportato verso Google Earth per ottenere una rappresentazione spaziale. Non finisce qui: inSSIDer è anche l'unico strumento del genere perfettamente compatibile con le architetture a 64 bit e funziona perfettamente sia con Windows Vista che con Windows 7.

Gli utilizzi possibili di uno strumento del genere sono i più svariati e passano dall'ovvio wardriving alla ricerca di reti wireless ai limiti del loro raggio d'azione, dal controllo delle inevitabili reti di terzi che invadono i nostri spazi fino all'ottimizzazione delle trasmissioni del nostro router. Proprio quest'ultima attività lo rende indispensabile a chi desidera ottenere il massimo dalla wireless LAN perché non diventa più necessario convincere il nostro sistema operativo a cercare continuamente nuove reti: inSSIDer lo fa per noi in automatico. In più la sua analisi di segnale è dettagliata e continuamente aggiornata e ci permette di posizionare il nostro router Wi-Fi in modo ottimale, mostrandoci le differenze di ricezione dovute anche all'orientamento di una singola antenna.

DA INTERPRETARE

Al di là degli schemi grafici con l'andamento della potenza del segnale in base al tempo e con l'occupazione di canali di ogni trasmissione, utili ma piuttosto semplici da interpretare, la vera forza di inSSIDer sono i dati numerici che ricava da ogni collegamento alle reti Wi-Fi. In modo particolare, il programma si distingue dai concorrenti per un'accuratezza elevatissima nel determinare l'RSSI, la forza di ricezione di un segnale in dolby. Questa va da 0 (massima potenza) fino a -100, quando Windows stesso non segnala più la rete. A tal proposito è in questi casi che si capisce che inSSIDer bypassa il sistema operativo: se anche Windows non riesce a segnalare una rete Wi-Fi, il programma riesce comunque a rilevarla, a calcolarne il segnale e a fornirci informazioni. Girando per casa con un portatile, per esempio, noteremo che il valore 0 è del tutto ipotetico e la maggior parte delle volte avremo un RSSI attorno al 50. Nel caso in cui usassimo un repeater, inSSIDer rileverà anche quello, come se fosse una rete separata ma con le stesse caratteristiche di quella reale.

Agendo opportunamente sul router Wi-Fi e sulle sue antenne, il programma ci mostrerà un riscontro immediato della situazione, permettendoci di ottenere una wireless lan ottimizzata nei dettagli.

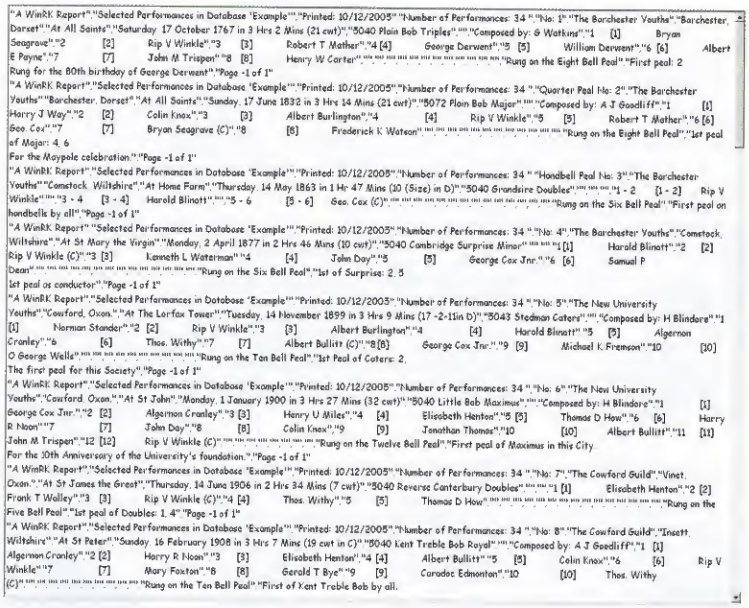
Aree Wi-Fi: trovarle è un gioco da ragazzi e il cartello è totalmente superfluo. Con inSSIDer bastano pochi secondi.

I dispositivi certificati sono i più affidabili e anche i più facili da trovare. Ma InSSIDer trova anche quelli "pirata".

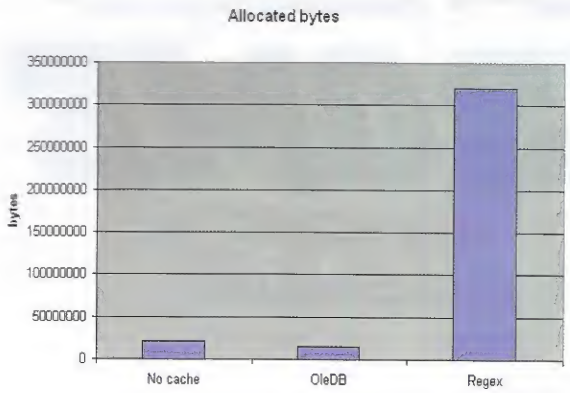
PROGRAMMING

NEL CD

PARSING CSV



"A WinRK Report","Selected Performances in Database 'Example'","Printed: 10/12/2005" "Number of Performances: 34 ","No: 1","The Barchester Youths","Barchester, Dorset","At All Saints","Saturday. 17 October 1767 in 3 Hrs 2 Mins (21 cwt)","5040 Plain Bob Triples","","Composed by: G Watkins","1 [1] Bryan Seagrave","2 [2] Rip V Winkle","3 [3] Robert T Mather","4 [4] George Derwent","5 [5] William Derwent","6 [6] Albert E Payne","7 [7] John M Trispen","8 [8] Henry W Carter","","","



Il metodo usato da DLL Helper, No Cache, usa una quantità di memoria bassissima, paragonabile al vecchio OleDB.

Manca totalmente la tipizzazione dei dati, solitamente affidata a istruzioni esterne al file oppure affrontata in modo brutale, con conversioni di massa al formato text. Allo stesso tempo esistono diverse varianti: alcuni programmi usano le virgole, altri il punto e virgola (Microsoft in testa), mentre altri ancora usano altri caratteri di interpunzione. Allo stesso tempo ci possono essere confusioni tra la virgola come delimitatore di campo, per esempio, oppure la virgola all'interno di un dato di testo, così alcuni delimitano i testi con le doppie virgolette mentre altri le usano singole.

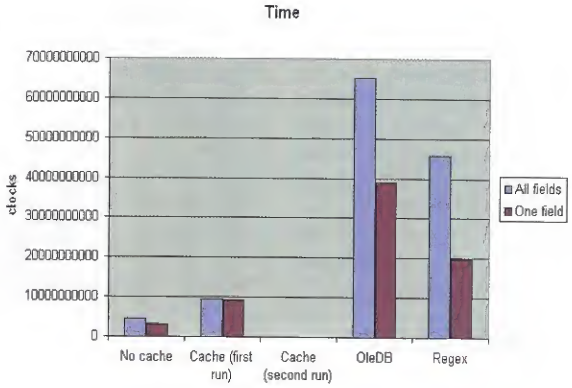
L'insieme delle regole, tuttavia, è limitato e non è difficile creare programmi, in qualsiasi linguaggio, capaci di interpretare correttamente un CSV generato da un'applicazione specifica. In più, non disponendo di strutture descrittive, quasi tutta l'informazione contenuta in un file (virgole escluse) è usata per trasmettere i dati. Essendo semplici file di testo, possono essere trasmessi con compressioni elevate, possono essere spezzati tra le righe per avere file più piccoli, non hanno limiti strutturali di dimensione perché non hanno alcuna struttura.

MASSIMA PERFORMANCE

Se, come abbiamo visto, la loro generazione non dà alcun problema di performance, la loro lettura può diventare un problema nel caso di file di grandi dimensioni. Per fare il parsing di un CSV, infatti, occorre leggerne una riga per volta, separare i campi con un'operazione di split sui separatori, intercettando le eccezioni per cui potremmo avere separatori all'interno di campi di testo. A questa operazione occorre aggiungere anche la trasformazione del dato isolato, solitamente di tipo testo, nel tipo necessario alla nostra applicazione.

Occorrono ottimizzazioni piuttosto estreme per portare questo processo ai livelli di efficienza necessari per il trattamento di migliaia di record. Per questo motivo, molti programmatori creano una propria libreria di parsing CSV che adattano ai loro vari progetti con un approccio che, tuttavia, fa spesso perdere tempo. Una soluzione già pronta e decisamente sofisticata, realizzata per i programmatori .Net ma aperta a ogni conversione, è stata realizzata da Sebastien Lorion che l'ha pubblicata, ormai qualche tempo fa, su codeproject.com: A Fast CSV Reader. Oggi è indicata come una libreria ormai standard, indispensabile nella cassetta degli oggetti di qualsiasi programmatore .Net, a qualsiasi livello. Il trucco usato da Sebastien è visibile a tutti grazie alla disponibilità del sorgente: gli serviva un reader di tipo forward-only il cui funzionamento andasse a interferire il meno possibile con il consumo di risorse.

La soluzione è stata quella di ricorrere alla classe System.IO.StreamReader, applicando varie regole di riconoscimento per i dati all'interno del CSV e cercando di ottimizzare il tutto. I risultati sono enormi: nel suo articolo afferma di raggiungere velocità di parsing 15 volte superiori ai metodi basati su espressioni regolari (regex) e noi confermiamo che la velocità varia, a seconda della complessità dei dati, da 13 a 16 volte quella dell'uso di regex. Pur preferendo la versione non cached, dalle performance superiori, Sebastien ha incluso nei download anche una versione cached. Unico neo della libreria, in entrambe le versioni, è l'impossibilità di fare un binding complesso dei dati con System.Web.UI.WebControls.DataGrid e System.Web.UI.WebControls.GridView. Quindi dovremo ricorrere a qualche trucchetto per collegarli a una GridView o a una DataView, perdendo però performance. Probabilmente la soluzione ideale sarà quella di usare il parser per quello che è: un metodo di input dei dati che poi vengono inseriti in un DB e consultati in seguito, con letture da DB e non da CSV.



I cicli di clock consumati da OleDB e da Regex per il parsing sono uno sproposito rispetto al parsing operato da questa libreria.

INTERNET

CHROME 10 BETA

LA NUOVA BETA DI CHROME LASCIA NELLA POLVERE LA CONCORRENZA GRAZIE A UN NUOVISSIMO MOTORE JAVASCRIPT.

di M.Brasile
redazione@hackerjournal.it

Chrome conquista sempre maggiori quote, erodendo sia il mercato di Internet Explorer che dello stesso Firefox, antagonista per eccellenza del browser di Redmond.

Il segreto di questo successo, oltre che nel marchio di Google, è da ricercare nell'estrema velocità e leggerezza che lo contraddistingue sin dalla versione di esordio. Unita a una notevole semplicità d'uso. Ma Google promette di fare molto di più, agendo sulle componenti base del Web come lo conosciamo per offrire un'esperienza sempre più entusiasmante ai suoi navigatori. L'ultima beta a disposizione (10.0.648.119) permette di provare l'ebbrezza del nuovo motore javascript che è del 66% più rapido del precedente! Scopriamo insieme le caratteristiche.

CARATTERISTICHE

Per provare Chrome, abbiamo bisogno di una macchina basata su Intel sulla quale giri un moderno sistema operativo. Tra quelli consigliati abbiamo:

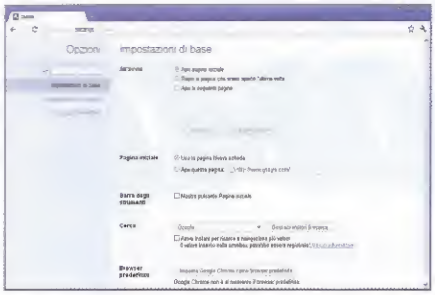
- Mac OS X 10.5.6 o superiore
- Windows XP Service Pack 2+
- Windows Vista
- Windows 7
- Ubuntu 8.04 o superiore
- Debian 5
- OpenSuse 11.1
- Fedora Linux 10

Lanciamo l'installer, o effettuiamo l'upgrade di un'installazione Chrome pre-esistente (aprendo direttamente il link http://www.google.com/intl/en/landing/chrome/beta) e siamo pronti a valutare il nuovo prodotto. La prima cosa che colpisce di Chrome è la sua interfaccia minimalista. Questo approccio è legato alla sintesi estrema dei comandi base di un'interfaccia verso il Web. La stessa barra degli indirizzi è in pratica una scorciatoia verso Google, il motore di ricerca, tanto che se digitiamo alcune parole invece di un indirizzo Web, verremo portati sulla pagina dei risultati della ricerca come se l'avessimo fatta su www.google.com.

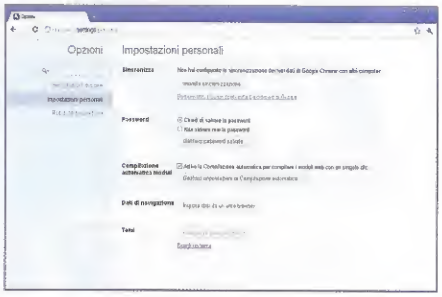
Man mano che visitiamo siti Web, vengono create delle miniature che saranno utilizzate poi per rappresentare la cronologia della navigazione, conservate nel caso in cui marchiamo con una stelletta (in alto sulla barra degli indirizzi) quelli che consideriamo "Preferiti".

NOVITÀ

Chrome 10 Beta, al pari delle versioni precedenti è veloce, semplice e stabile. Ha a disposizione l'opzione per una navigazione privata (in cui vengono eliminati cookies e tracce residue che potrebbero essere altrimenti usate dai siti Web) e per l'utilizzo offline di applicazioni Internet.
In particolare si parla di Google desktop e anche di una comoda funzione di ricerca di testo all'interno delle pagine contenute nella cronologia della navigazione.
Dobbiamo dire che manca un blocco per banner pubblicitari e forse la gestione dei bookmark non è così semplice come vorremmo. Manca anche un supporto diretto ai feed RSS, come siamo abituati ad avere con Firefox e c'è da dire che vengono utilizzate notevoli risorse di sistema.
Ma nonostante questi nei, Chrome riesce a stabilire un incredibile primato grazie al nuovissimo motore interno V8, chiamato Crankshaft (letteralmente "albero a gomiti") dedicato alla gestione dei javascript. Viene infatti valutato del 66% più



Le impostazioni di Chrome sono così aumentate da richiedere pagine dedicate. In quelle base abbiamo tutti i settaggi di carattere generale ma il livello di dettaglio può essere elevato.



Nelle impostazioni personali troviamo la nuova capacità di sincronizzare più installazioni di Chrome, tramite account Gmail: non dovremo più preoccuparci di bookmark e password.

performante della precedente versione di Chrome utilizzando V8 Benchmark Suite - version 6, un tool realizzato proprio da Google per misurare le prestazioni dei browser (http://v8.googlecode.com/svn/data/benchmarks/v6/run.html).

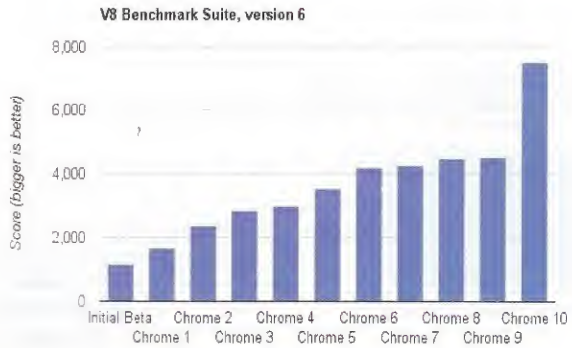
Qualcuno potrebbe obiettare che non è attendibile un confronto fatto "in casa" da Google, ma le prestazioni di Chrome 9 in effetti vengono battute al momento solo da Chrome 10 beta!

E oltre alle prestazioni così elevate raggiunte nell'esecuzione del javascript, si aggiunge il supporto preliminare alla capacità di sfruttare l'accellerazione di calcolo delle moderne schede video, al cui interno sono montati processori dedicati chiamati GPU (Graphic Process Unit). Questa abilità permette di risparmiare fino all'80% delle risorse CPU utilizzate normalmente quando navighiamo in full-screen, con benefici diretti oltre che nel rendering delle pagine, anche sulla maggior durata delle batterie se ad esempio usiamo un notebook.

È cambiata la gestione delle impostazioni che ora compaiono in un nuovo tab dedicato, permettendo di osservare tutto in modo più agevole rispetto al box che compariva precedentemente.

La cosa interessante è che è stata integrata una barra di ricerca nelle opzioni, così se non siamo sicuri di che cosa stiamo cercando è Chrome stesso ad aiutarci indicandoci dei risultati collegati alle parole chiave che abbiamo inserito. E i risultati non sono semplici link, ma direttamente le opzioni che vogliamo poi modificare così da rendere i cambiamenti immediatamente attivi appena le spuntiamo.

Un altro meccanismo interessante riguarda la disattivazione automatica dei plugin nel momento in cui scadono, fintanto che non vengono aggiornati. Questa caratteristica impatta direttamente sulla sicurezza, perché spesso i cosiddetti exploit dei pirati informatici sfruttano proprio la vulnerabilità di funzionalità non manutenute come possono essere quelle di plugin non più aggiornati e dimenticati, per pigrizia o per ignoranza, installati e attivi.



L'incremento delle prestazioni di Chrome 10 rispetto alla 9 e alle precedenti è esponenziale! Per verificare che sia vero basta installarlo e provarlo di persona.

Un'altra interessante funzionalità è rappresentata da Chrome Sync, che permette di controllare la configurazione di più installazioni di Chrome, condividendo password e bookmark, preferenze, temi ed estensioni. Per maggior sicurezza, viene implementato un sistema di criptaggio delle password basato su una frase di sblocco (passphrase).

Infine, al pari di Firefox, i nuovi tab possono essere aperti senza spostare il focus dalla finestra corrente

GIUDIZIO

Nonostante si tratti di una beta, il funzionamento sembra davvero affidabile nei test che abbiamo fatto. Anzi, utilizzare la nuova versione non fa rimpiangere alcuna delle precedenti tanto da invogliarci a effettuare un downgrade (dal momento che si tratta di una beta tuttavia, è possibile disinstallarla e tornare a una precedente versione stabile dato che i programmi vengono caricati in cartelle differenti). Il nuovo motore V8 è indubbiamente la punta di diamante e sarà duro per la concorrenza riuscire a ottenere risultati comparabili. Google investe molto su questa tecnologia, dato che ha scelto di implementarla in tutte le sue applicazioni Web ed è possibile che in futuro nessuno dei competitor riuscirà a strappare simili primati se non iniziano subito a recuperare terreno. Restano ancora dei nei che possono trattenere i più dall'abbandonare Firefox (basti pensare alla vastità di plugin disponibili e la quantità di aggiornamenti costanti rilasciati). Senza paragone invece il confronto con Internet Explorer che sembra perdere smalto al confronto di Chrome.

Non possiamo prevedere cosa accadrà nell'immediato futuro, ma Chrome ha sconvolto sicuramente gli equilibri di un mercato che sembrava ormai cristallizzato.

INTERNET

CHROME WEB STORE

IL NUOVISSIMO NEGOZIO ONLINE DI GOOGLE, DOVE È POSSIBILE ACQUISTARE LE APP PER CHROME.

di M.Brasile
redazione@hackerjournal.it

Nel mondo di Internet si sa che le novità sono quotidiane, ma non sempre sono tali da avere risvolti epocali come quando escono dal cappello di Google. L'ultima sorpresa presentata ufficialmente da Big-G è un negozio online interamente dedicato alle applicazioni e ai plugin che è possibile installare sul suo browser Chrome e in futuro che si potranno installare su Chrome OS.

Il bello è che la maggior parte delle applicazioni sono completamente gratuite, anche nel caso in cui siano realizzate da partner commerciali! Scopriamolo insieme.

REQUISITI

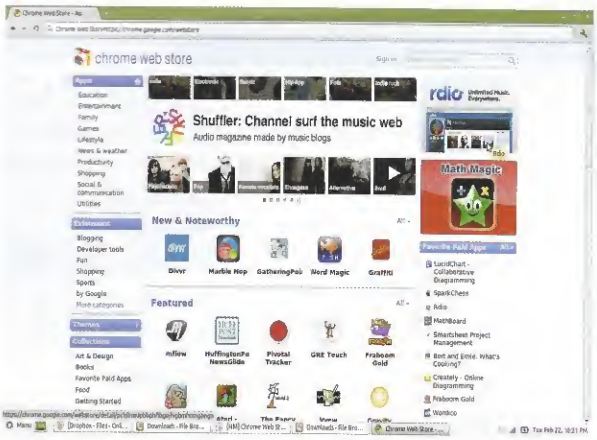
Non sarebbe nemmeno necessario indicare il link di Chrome Web Store (https://chrome.google.com/webstore, importante httpS davanti), dato che cercandolo sulla barra di Google è ovviamente il primo risultato trovato. Ma se lo apriamo con Firefox, Internet Explorer o qualunque altro browser che non sia Chrome veniamo subito avvisati che per poter accedere al negozio occorre farlo proprio con lui (unico navigatore supportato al momento).

Quindi se non lo abbiamo già sulla nostra macchina, dobbiamo scaricarlo e installarlo, ma si tratta di una procedura davvero semplice: con un browser qualunque apriamo l'indirizzo www.google.com/chrome e premiamo sul grande pulsante blu "Scarica Google Chrome".
Terminato il download del file lo lanciamo e l'installer completerà la procedura in breve in modo automatico.

ORGANIZZAZIONE

Avere a disposizione un unico punto di riferimento da cui attingere è sicuramente una grande comodità, ma si è voluto superare anche la questione sicurezza che impatta ogni volta che sul pc di un utente si va ad aggiungere un nuovo software: installare più di un plugin tramite il Web Store invece permette di richiedere l'autorizzazione un'unica volta e lasciare all'utente solo il piacere di scegliere cosa installare, senza eccessivo disturbo. Per procedere è necessario infatti creare un account su Google (nel caso non si possedesse già ad esempio un indirizzo su Gmail che va benissimo), per autenticarsi e procedere. Se non lo facciamo subito, ci verrà richiesto nel momento in cui vogliamo installare qualcosa dallo Store.

Apriamo dunque il Web Store e la prima cosa che ci colpisce sono le icone colorate delle App proposte, in uno stile che ricorda molto da vicino quello dell'App Store di Apple. C'è un'area promozionale dove scorrono le App suggerite, poi tutto intorno abbiamo diversi modi per fare ricerche per aree. Se invece vogliamo andare a cercare qualcosa in particolare, usiamo la barra di ricerca (poteva mancare sul negozio di Google?) che troviamo in alto a destra. Al centro tro-



App, estensioni, temi e collection: un unico punto di accesso a una miniera di risorse per arricchire il browser. Esattamente come avviene per altri blasonati prodotti.

viamo immediatamente delle App più interessanti che hanno ovviamente il maggior risalto, o perché commerciali o perché appena rilasciate online. Lateralmente troviamo diversi menu che ci aiutano a trovare le App secondo classificazioni logiche.

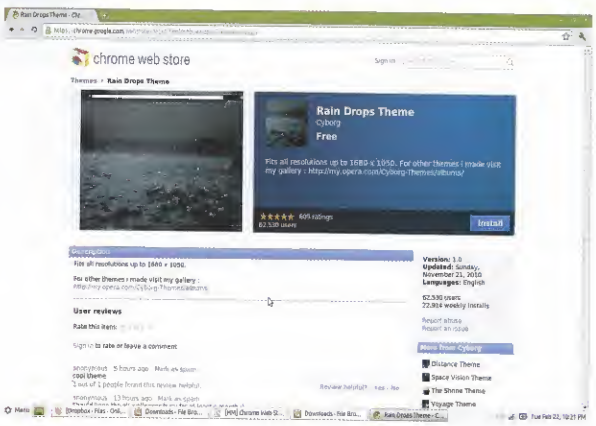
Possiamo così identificare subito che cosa ci interessa, scegliendo tra Apps (applicazioni vere e proprie), Extensions (i cosiddetti plugin del browser che ne aumentano o modificano le funzionalità), Themes (i temi grafici che cambiano l'aspetto di Chrome), Collections (che è un modo diverso di classificare le App basandosi su tematiche). Troviamo poi sulla destra una classifica delle App più apprezzate (Top rated). Per ogni App possiamo visualizzare un fumetto con le informazioni principali semplicemente passandoci sopra con il puntatore: se gratuito (free) o a pagamento, quanti utenti l'hanno già scaricato, una breve descrizione dello scopo e utilizzo, l'autore e delle stelline che riassumono i diversi feedback che hanno dato gli utenti che lo hanno già usato.

LE APP

Le App vere e proprie sono classificate in diverse categorie:

- Education: materiale didattico, adatto sia ai piccoli e piccolissimi, che ai ragazzi e studenti (ad esempio possiamo trovare un planetario, una lavagna scolastica sulla quale imparare la matematica, animazioni per i piccini e tanto altro)
- Entertainment: questa è una categoria abbastanza vasta che è adatta a ogni età e permette di scegliere tra programmi di musica, televisione, fumetti, notizie, e utility divertenti; non mancano anche giochi evoluti, come quelli di ruolo
- Family: qui iniziamo a vedere argomenti trasversali che possiamo trovare anche nelle altre aree, ma che hanno chiaramente come target principale tutta la famiglia o i piccoli (come musei virtuali dedicati alla preistoria, gli oceani, il corpo umano e così via)
- Games: non può mancare la categoria dedicata a tutti i tipi di giochi Arcade & Action, giochi di carte, mondi virtuali, giochi di ruolo, giochi di abilità, giochi sportivi e giochi popolari
- Lifestyle: qui troviamo app per un pubblico più adulto e interessato ad aspetti legati allo stile di vita (come arredamento, moda, fitness e via dicendo)
- News & Weather: immancabilmente, le notizie e il meteo sono tra gli argomenti più gettonati per un plugin e dato che possono arrivare da siti, feed, blog, facebook... ci sono moltissime diverse App per organizzare e leggere le notizie
- Productivity: quando abbiamo bisogno veramente di un programma utile, dobbiamo cercarlo in questa categoria che raccoglie gli strumenti che possono facilitarci la vita di tutti i giorni, ad esempio per gestire i conti di casa, scrivere qualche nota o appunto, ma persino software per leggere file e pagine Web e creare registrazioni audio automatiche
- Shopping: se non esistesse lo shopping internet sarebbe ancora utilizzato solo nelle università, invece esistono molti siti di e-commerce come eBay e Amazon che possono essere più facilmente gestiti tramite qualche App dedicata
- Social & Comunication: tutto ciò che gravita intorno alla messaggistica e ai social network, si incontra nei modi più diversi; ecco quindi arrivarci in aiuto una serie di app dedicate a questi mondi che permettono di integrarli in Chrome e avere tutto a portata di click
- Utilities: ciò che è veramente utile (ma anche tutto quello che risulta totalmente inutile) e di cui una volta installato non possiamo più fare a meno di usare lo troviamo in questa categoria.

Le schede dei prodotti sono complete e ricche di dettagli. Sarà comunque nostra cura controllare che le caratteristiche siano compatibili con la nostra configurazione. Nel caso dei temi, per esempio, le dimensioni del nostro monitor restringeranno o amplieranno il campo della nostra ricerca.



LE ESTENSIONI

Quello che era in origine il plugin viene chiamato estensione in Chrome, richiamando il significato più ampio del termine, ossia quello di aumentare le funzionalità del browser di base. Quindi se un App può girare anche su un sito online, l'estensione tipicamente gira proprio sul nostro browser.

Le categorie in cui sono divise le estensioni (extensions) sono:

- Blogging: dedicato ai blog, a twitter e a tutti gli strumenti che si basano su questa modalità di fare Web, come la condivisione dei documenti e dei link
- Developer tools: gli strumenti per sviluppatori, utilissimi per chi programma, ma anche per chi è curioso di scoprire come è fatta una certa pagina o una certa soluzione; troviamo però anche utilità per chi si occupa di grafica o di posizionamento sui motori di ricerca
- Fun: si tratta di strumenti dedicati al divertimento, più che all'utilità infatti sono dei passatempi che possiamo usare su Chrome e Internet; ma possiamo trovare anche strumenti interessanti come StumbleUpon che riesce a trovare per noi gli argomenti più dibattuti sul Web
- Shopping: creare una seconda area dedicata allo shopping la dice lunga sugli interessi dietro a uno Web Store! Diciamo che in questa però troviamo estensioni un pò più tecniche di quelle presenti nella categoria delle App
- Sports: per gli appassionati di qualunque sport, è possibile trovare un'estensione per ogni gusto, per seguire le classifiche e gli eventi sportivi (in particolare americani)
- by Google: qui troviamo estensioni create e promosse proprio da Google; sono quelle consigliate a tutti, da provare e valutare personalmente
- Accessibility: queste estensioni sono dedicate a chi ha problemi di vista e magari vuole avere il testo più grande, o una tastiera sullo schermo, o uno zoom dinamico da comandare all'occorrenza, così come poter cambiare il contrasto cromatico o l'intera rosa dei colori usati
- News & weather: come per l'omonima nelle App, è dedicata agli argomenti più interessanti di sempre
- Photos: navigando possiamo raccogliere molte immagini e foto che magari vogliamo conservare e consultare, condividere e modificare e in questa categoria troviamo molti strumenti dedicati
- Productivity: come per le App, nelle estensioni possiamo avere degli strumenti che ci facilitino le diverse cose che possiamo fare online, come catturare immagini dei siti web che ci interessano maggiormente, stampare in pdf, usare un dizionario, bloccare dei siti Web dai risultati di Google
- Search tools: riuscire a trovare le informazioni può non essere facile, anche se usiamo Google e abbiamo una certa esperienza; grazie a queste estensioni però possiamo evidenziare alcuni risultati, le parole chiave, i siti più interessanti o più simili a quelli che ci interessano. Anche queste estensioni meritano di essere provate sul campo per farsi un'idea di cosa è possibile avere con le moderne tecnologie
- Social & communication: di nuovo, social network e messaggistica, visti però dal punto di vista dei plugin per Chrome

TEMI

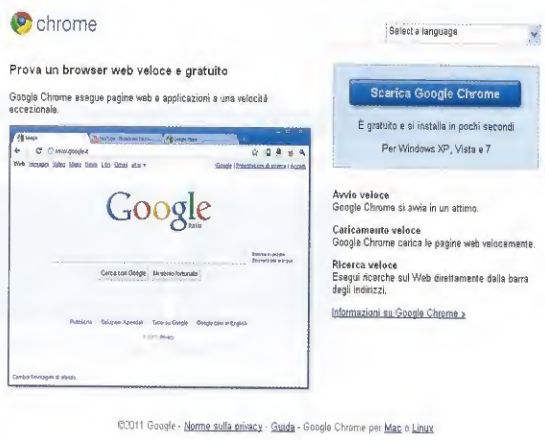
Già da tempo Chrome ci ha abituato alla possibilità di cambiare aspetto, al pari di Firefox e altri browser. Non poteva quindi mancare anche un'intera area del Web Store dedicata unicamente ai temi che possono essergli applicati.

Possiamo scegliere tra gli ultimi arrivi e tra quelli più popolari e per ciascun tema ci viene indicato il numero di quanti utenti lo hanno già scaricato.

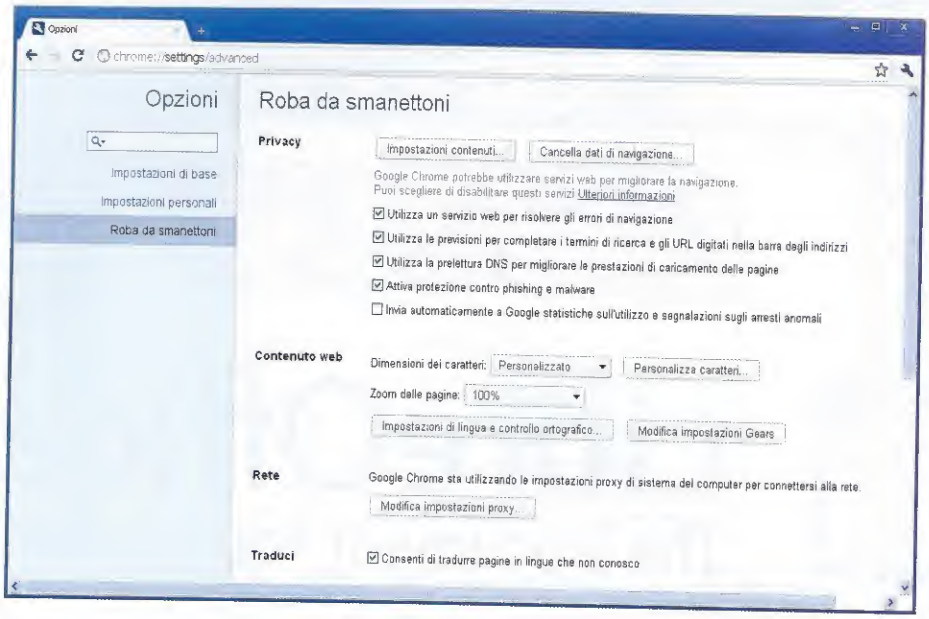
COLLEZIONI

Le stesse App e Extensions possono essere catalogate in modo tematico. Troviamo quindi una classificazione diversa rispetto a quella già vista che presenta queste scelte:

- Art & Design: in questa sezione troviamo tutti i prodotti dedicati all'arte, al disegno e alla grafica in generale
- Books: tutto quello che è dedicato ai libri, reali o virtuali e ai negozi collegati a questo business
- Favorite Paid Apps: tutte le migliori App commerciali, il che non vuol dire necessariamente che siano a pagamento anzi... sono quasi tutte completamente gratuite o in alcuni casi prevedono il pagamento tramite la App stessa
- Food: le App dedicate all'alimentazione e alla ristorazione
- Getting Started: queste possono essere considerate le App che lanciamo non appena ci colleghiamo a Internet, per cercare le ultime notizie, ascoltare un po' di musica, leggere i tweet o fare acquisti su eBay
- Money: programmi di tutti i tipi per la gestione dei conti personali



In piena filosofia Google, che ha fatto della sua scarna homepage una bandiera, persino l'invito a provare Chrome è decisamente sottotono rispetto alle sue potenti caratteristiche.



Cosa fare tra un sito e l'altro? Giocare, ascoltare musica o usare una delle tante app che Google ci mette a disposizione per Chrome. Oppure apriamo un'altra finestra e sfogliamo il catalogo.

• Music: una raccolta di tutte le App dedicate alla musica, da ascoltare, da suonare e da condividere
• New & Noteworthy: una categoria variegata con App che non è facile classificare data l'originalità
• Photos: tutti gli strumenti dedicati alla visualizzazione,alla modifica e condivisione delle foto
• Presentation Tools: tanti strumenti utili per creare slide show e presentazioni ovunque ci troviamo
• Sports: il mondo degli sport, nessuno escluso, da tutti i punti di vista
• Staff Picks: le scelte dello chef, o meglio dello staff che lavora nel Web Store; praticamente perfette sono assolutamente da provare, almeno una volta.
• Students: i materiali didattici e le app più adatte agli studenti trovano posto in questa categoria
• TV & Movies: televisione e film e tutto ciò che gli gravita intorno (programmazioni, recensioni, streaming, ..)

CONSIDERAZIONI

Google si sa, sta puntando sulle applicazioni Web da tempo e il futuro sistema operativo Chrome OS sfrutterà a dovere il canale del Web Store. Intanto grazie a Chrome, Google può promuovere una piattaforma di software a pagamento da acquistare tramite Google Checkout e creare una solida base di nuovi clienti per le future App, previste per il prossimo sistema operativo.
In questo modo, il nuovissimo Web Store potrebbe diventare il portale di accesso dei prossimi computer venduti con Chrome OS, o semplicemente una vetrina a cui accedere dal PC, notebook, netbook o smartphone con sopra Android. Google saprà stupirci ancora e questo, siamo convinti, è soltanto la punta di un iceberg di novità in arrivo.

Store sempre più esclusivi?
Apple, Nokia, Microsoft, ora anche Google e poi mille altri: gli store spuntano come funghi in ogni angolo del Web. Praticamente qualsiasi produttore di hardware o software tenta di confinarci all'interno del suo negozio privato, raccontandoci che dispone di milioni di applicazioni, di miliardi di utenti, che il suo store è il più bello, il più buono, il più bravo.
Dietro ci sono logiche di marketing enormi che portano questi colossi a scontrarsi e ribattendo colpi su colpi. Per fortuna, però, non tutti fanno come Apple (ve lo ricordate lo slogan "Think Different"? Oggi sembra essere "Think Closed") che rende blindato il suo hardware incollando gli utenti al suo Apple Store e costringendo chi desideri un minimo di libertà a infrangere le regole e invalidare la garanzia in una sorta di ricatto legale.
La maggior parte degli store, per fortuna, accetta la concorrenza di altri siti e non si propone come dirigente esclusivo della vita informatica di acquirenti di hardware e software. Il Chrome Store ci piace molto, così come ci piacciono i repository centralizzati per Firefox e altre soluzioni Web fatte per semplificarci la vita. Speriamo, però, che il caso di Apple sia l'eccezione e che gli altri non la seguano su questa strada. Speriamo che gli indecisi, come Nokia, favoriscano la diffusione delle applicazioni anche con altri sistemi, come blog e siti indipendenti.

LIBRE OFFICE

LibreOffice
The Document Foundation

HANNO PROVATO A CHIUDERE OPENOFFICE, MA È NATO LIBREOFFICE!

di M. Brasile
redazione@hackerjournal.it

Forse non tutti sanno che Oracle ha acquisito Sun e con essa anche OpenOffice, il software open-source finanziato dai creatori di Solaris e Java che è diventato l'unico vero concorrente di Microsoft Office.

Nell'ultima versione di OpenOffice è ben visibile il logo di Oracle. Oracle, un colosso del settore IT al pari di Microsoft, ha chiaramente mire commerciali e la comunità degli sviluppatori di OpenOffice è rimasta abbastanza scossa dalla vendita di Sun, non potendo conoscere le loro intenzioni nei confronti di prodotti mantenuti finora gratuiti. Basti pensare che MySql, il motore per database gratuito per eccellenza e oggetto di investimenti da parte di molte aziende, risulta acquistato da Oracle, a seguito dell'acquisizione di Sun e avrà sicuramente le sorti segnate, a favore dei prodotti per database che hanno reso famosa Oracle.

A seguito di questo evento finanziario, dagli sviluppi tetri e oscuri per la community, a fine 2010 è nato un progetto completamente nuovo chiamato LibreOffice (www.libreoffice.org), sponsorizzato da The Document Foundation, un consorzio di aziende da tempo nel campo open-source come Red Hat, Ubuntu e persino Google. Grazie a questi sostenitori, si può dire che LibreOffice sia il nuovo prodigio sulla scena Internet, dato che è fornito a costo zero e i suoi sviluppatori sono stati abbastanza impegnati per pubblicare la prima major release 3.3 alla fine dello scorso gennaio. Nel momento in cui scriviamo è uscito il primo aggiornamento, è quindi possibile installare LibreOffice 3.3.1.

Questo stesso articolo è stato scritto con LibreOffice: non appena è uscito non potevamo che correre a provarlo!

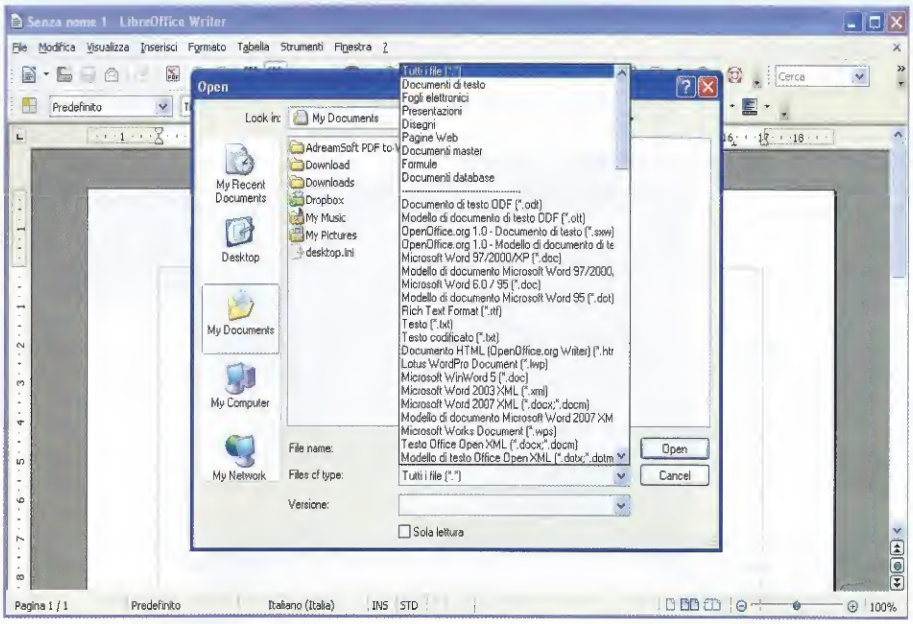
CARATTERISTICHE

Per chi non conoscesse affatto OpenOffice, possiamo dire che si tratta (o dovremmo dire si è trattato?) di una suite completa alternativa a Microsoft Office, grazie alla quale è possibile creare lettere, documenti, report, pagine web, fogli di calcolo, analisi dei dati, creazione e modifica di disegni, loghi, diagrammi di flusso, etichette, biglietti da visita, presentazioni, gestioni di database e quant'altro venga in mente, in modo completamente gratuito dato che il software è open-source. LibreOffice riprende completamente in mano il progetto, assicurando continuità nello stile open-source.

LibreOffice è una suite di programmi che spaziano dalla videoscrittura, alla gestione di fogli di calcolo e presentazioni.

La suite è composta da diversi software:

- **Base**, per la gestione dei database
- **Calc**, per i fogli di calcolo
- **Draw**, per il disegno e grafica decorativa
- **Impress**, per le presentazioni
- **Writer**, per la videoscrittura
- **Math**, per la scrittura di formule matematiche perfette dal punto di vista grafico



Writer clona Word, anche se è più simile a Word 97 che al 2007. Nell'immagine è possibile vedere tutti i formati supportati, tra cui anche quelli più recenti. Senza mai trascurare la compatibilità.

Ogni programma può essere richiamato separatamente, ma da ciascuno è possibile aprire i file degli altri permettendo di dimenticarci se abbiamo aperto Calc invece di Writer ad esempio e lavorare comunque con l'ambiente di lavoro giusto.

INSTALLAZIONE

A differenza di OpenOffice, che grazie alla diffusione che aveva raggiunto era rilasciato già compilato per le diverse lingue, e svariati mirror in tutto il mondo, con LibreOffice dobbiamo procedere a installare due pacchetti: LibreOffice vero e proprio e l'aggiornamento separato per la guida italiana (chiamato help pack). Se non installiamo il secondo pacchetto, cliccando su Aiuto saremo indirizzati alla guida online nel sito di LibreOffice. Può non essere obbligatorio quindi, se siamo sempre connessi a internet, ma può capitare che non abbiamo il collegamento e magari vogliamo approfondire qualche nuovo comando o ci occorre un po' di aiuto per realizzare una funzione più complicata. A scapito di qualche megabyte, conviene quindi installare anche la guida. Passo fondamentale invece, per poter funzionare completamente è necessario che sia presente sulla propria macchina il Java Runtime Environment (JRE), non incluso nell'installazione.

Noi abbiamo usato l'ultima versione disponibile, la 6 aggiornamento 24, ma anche una precedente dovrebbe andare bene. Nel caso non abbiamo nulla già pronto, basta lanciare l'installer di JRE e accettare le impostazioni predefinite (in questo caso è probabile che sia necessario un riavvio della macchina prima di poter installare LibreOffice). Avendo già a bordo il JRE, l'installazione di LibreOffice procede poi senza intoppi sia su Windows XP, sia su Vista e Seven.

L'unica pecca riguarda la mancata cancellazione dei file temporanei dopo il setup, che dobbiamo quindi rimuovere manualmente (basta trascinare nel cestino la cartella temporanea che si crea nella cartella dell'installer).

Anche nell'ultima versione di Java Runtime Environment campeggia il logo di Oracle. Visti gli attuali interessi in gioco, sarà così a lungo.

Il wizard ci permette di vedere in un colpo solo tutti i programmi della suite. In alternativa, possiamo trovare i singoli programmi tra le applicazioni.

NOVITÀ E DIFFERENZE CON OPENOFFICE

Una volta completata l'installazione, lanciando LibreOffice vediamo la classica interfaccia cui siamo abituati con OpenOffice. In effetti, al primo impatto, è difficile trovare differenze dato che questa prima versione di LibreOffice riprende in pieno dove era arrivato l'altro progetto. Il lavoro è stato svolto andando a migliorare il codice (risolvendo bug o raffinando il programma) che forse si vede meno, ma rende l'applicazione più rapida e funzionale.

Tra le novità, nel **Writer** (il clone di Word) è possibile inserire immagini vettoriali (quelle con estensione SVG) ed è anche possibile modificarle tramite l'editor grafico chiamato **Draw**. Il formato SVG è particolarmente amato in ambito open-source, perché è uno standard aperto, ma in effetti è poco usato normalmente, tranne che nei web browser.

Un'altra caratteristica interessante, magari più per gli addetti ai lavori, riguarda la possibilità del Writer di caricare e salvare documenti in ODF (il formato aperto nato per contrastare i formati chiusi di Microsoft) come documento XML, il che semplifica le procedure di modifica. Sembrerebbe un fattore di poco conto, ma considerando che nel web è in atto una migrazione verso il formato XML, si può intuire che il futuro delle applicazioni come LibreOffice deve tenerne conto.

Inoltre, come già avveniva con OpenOffice, è in grado di importare file nel formato Lotus Word Pro ed è migliorata l'importazione del formato Wordperfect. È possibile aprire anche i file in formato Microsoft Works.

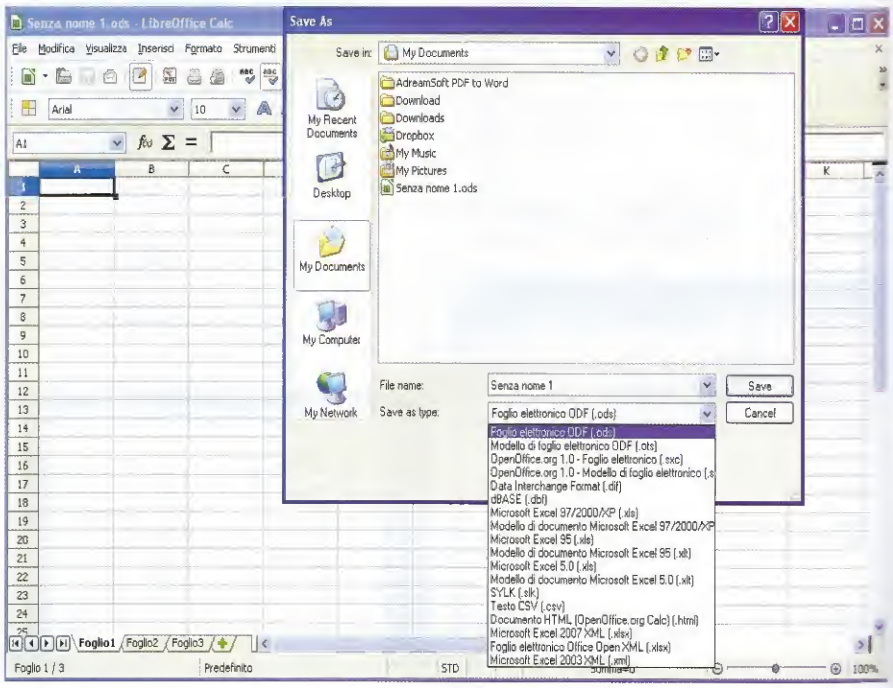
Una novità che resta invece più interessanti per la maggior parte degli utilizzatori è la migliore compatibilità offerta verso il formato di Microsoft Office 2007, che finalmente permette di gestire anche file complessi, pieni di commenti e revisioni, non possibile finora neanche con OpenOffice.

È stato poi migliorato anche il sistema di numerazione delle pagine e la finestra di dialogo per l'anteprima di stampa.

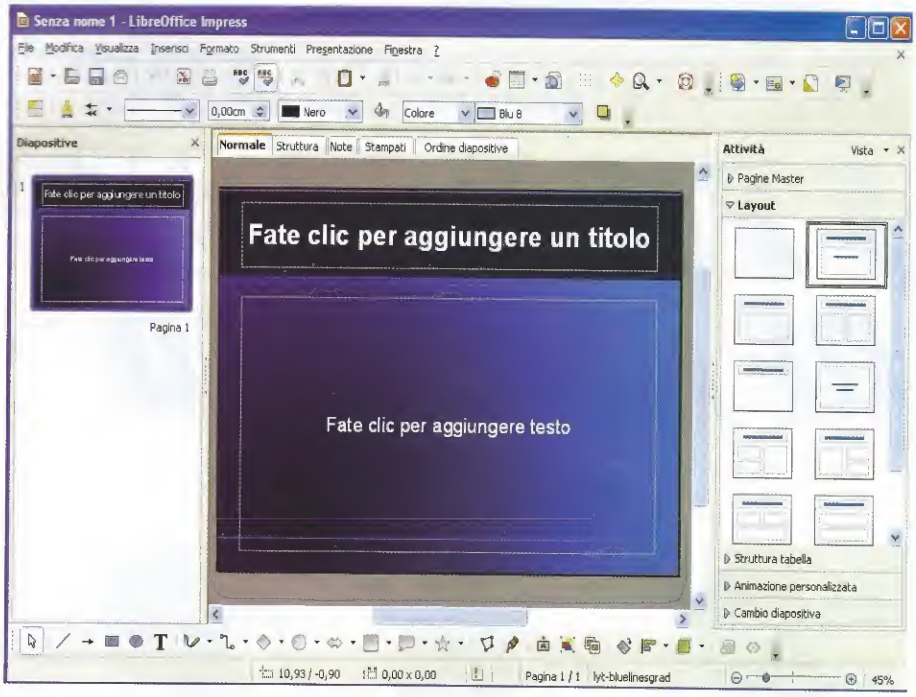
Per quanto riguarda Calc (il clone di Excel), viene introdotto il supporto di ben un milione di righe, che può essere ininfluente per gli utilizzi normali, ma rende l'idea dei progressi fatti. È possibile usare le stesse scorciatoie di Excel e le stesse convenzioni per le operazioni sulle celle. Restano ancora molte differenze, dato che non tutti i comandi di Excel sono ancora supportati.

Impress (il clone di PowerPoint) introduce diverse novità, tra cui Presenter Console che permette di semplificare la gestione delle presentazioni quando il laptop è connesso a un proiettore. Precedentemente era possibile averlo solo come add-on, ma non era così facile trovarlo e ora invece è parte integrante del programma. Offre inoltre una piena compatibilità con le presentazioni di PowerPoint, consentendoci di considerarlo una vera alternativa.

Nella suite sono presenti poi Base (che clona Access di Microsoft) e Math, un prodotto inedito che ha come unico scopo quello di realizzare perfette riproduzioni delle formule matematiche dal punto di vista grafico (compito arduo con Word ad esempio). Soprattutto gli studenti possono avvantaggiarsi di questo prodotto che è davvero semplice da usare. Per usarlo si può lanciare in modalità indipendente (dal menu ad esempio) o da dentro Writer inserendo una formula (Inserisci -> Oggetto -> Formula)



Calc è il clone di Excel e in effetti non c'è molta differenza per l'utilizzo abituale. Nell'immagine è possibile vedere tutti i formati supportati da questa versione.



A prima vista è difficile accorgersi che non si tratta di PowerPoint, dato che abbiamo lo stesso layout e le stesse funzioni con Impress. Utilizzandolo impareremo ad apprezzarlo presto.

GIUDIZIO

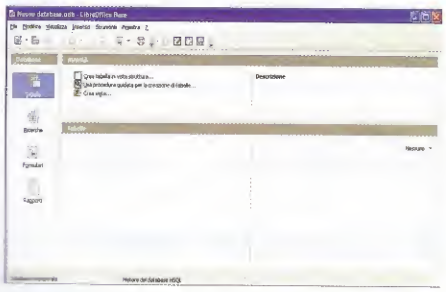
LibreOffice è affidabile, funzionale e gratuito. Con le migliorie apportate al codice è anche più veloce e presenta meno bug delle ultime versioni di OpenOffice.

Tuttavia la nuova gestione, che riporta alle origini di questa suite che per prima è riuscita a contrastare il monopolista del mercato, promette interessanti sviluppi che potrebbero in futuro ribaltare le posizioni di mercato.

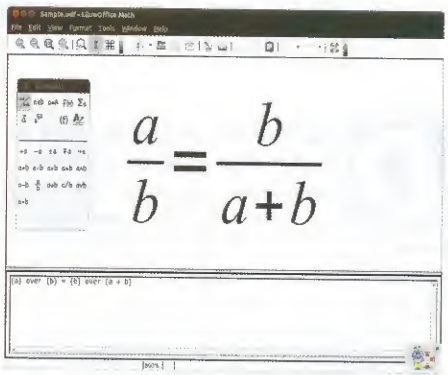
Il prodotto resta completamente gratuito e libero dalle linee guida di Oracle o di altri "proprietari" invadenti (la presenza di Google, al pari di ciò che è stato IBM per il kernel linux, rappresenta più una garanzia che un'ingerenza a giudicare dal supporto economico offerto gratuitamente senza incidere sulle scelte degli sviluppatori), il che permette di considerarlo tranquillamente per tutte quelle realtà in cui il fattore economico può fare la differenza (pensiamo alle scuole, alle onlus e all'associazionismo). Ma anche nel privato, si può utilizzare un prodotto gratuito per copyright, che funziona davvero e rende facile l'interscambio quotidiano di documenti.

LibreOffice nasce sotto una buona stella, coccolato sia dagli sviluppatori che dalle case open-source e non vediamo l'ora di seguirne i progressi.

Vi consigliamo di provarlo e giudicarlo con l'utilizzo normale, perché si tratta di un prodotto davvero valido. In casi come questo non è il prezzo che fa la differenza, ma la volontà e l'impegno di tantissimi programmatori sparsi in tutto il mondo accumunati tra loro da un progetto vincente.



Con Base possiamo gestire semplici database senza rimpiangere Access. Ha tutte le funzionalità base cui siamo abituati.



Grazie a Math non ci sono più problemi per disegnare formule matematiche identiche a quelle che scriveremmo su una lavagna.

HACKING
NEL CD

DISASSEMBLARE I FILE DEX DI ANDROID

IL FILE DEX CONTENUTO NEL PACKAGE APK CHE CORRISPONDE A UN APPLICATIVO ANDROID CONTIENE LA VERSIONE COMPILATA DELLE CLASSI JAVA DEL NOSTRO PROGRAMMA. SI PUÒ, A PARTIRE DAL FILE COMPILATO, TORNARE AL SORGENTE? QUESTO ARTICOLO DOCUMENTA LO STATO DELL'ARTE IN MATERIA.

di G.Enoma
redazione@hackerjournal.it

Disassemblare è un'arte. Arte faticosa che richiede impegno e dedizione, studio e intuizione, strumenti potenti e capacità di inventarne di nuovi. Per dedicarvi tante energie ci vuole un motivo. Potrebbe essere una necessità: dobbiamo accedere ai nostri dati e l'applicazione che li legge non è più supportata sul nuovo PC, oppure abbiamo perso il sorgente di quell'eseguibile creato tanto tempo fa, e di cui non abbiamo un backup. Potrebbe anche essere voglia di guardare "sotto coperta".

Ad esempio per sapere cosa fa il compilatore quando abilitiamo un suo certo flag di ottimizzazione e magicamente il nostro programma diviene più performante: capire cosa lui ottimizzi ci aiuta a scrivere programmi migliori. Ma sicuramente non è, per il modo di pensare Hacker, un modo per rubare. Rubare idee altrui che per qualunque motivo non sono rese pubbliche. Quindi, senza troppi giri di parole, disassemblare programmi altrui che non siano Open Source è reato.

DISASSEMBLARE, MA COSA?

In due precedenti articoli (HJ 208 e 209) abbiamo visto la struttura del sorgente di un'applicazione Android e quella del relativo pacchetto eseguibile (APK). Abbiamo in particolare imparato che il codice Java è codificato in un file con estensione DEX. Qui affrontiamo il tema di disassemblarne il contenuto.

LA DALVIK VIRTUAL MACHINE

Il sistema operativo Android usa una VM (Virtual Machine) per eseguire il codice delle sue applicazioni. Sebbene le applicazioni siano scritte in Java, la VM non è la classica JVM (Java Virtual Machine), bensì la DVM (Dalvik Virtual Machine). Per i più curiosi, Dalvik non è un eroe dei fumetti, ma semplicemente il nome di un villaggio di pescatori Islandese. La differenza per noi fondamentale è che la DVM non usa il bytecode Java, ma un formato specifico chiamato DEX. Prima di procedere è bene chiarire un concetto forse noto, ma che non fa male rinfrescare. Le istruzioni Java, come quelle di qualunque altro linguaggio di programmazione di alto livello, non sono eseguibili direttamente dal processore: devono essere tradotte in uno o più *opcodes* (Codici operativi). La corrispondenza non è "uno-a-uno", ma "uno-a-molti", ovvero ad ogni istruzione Java corrispondono una sequenza di istruzioni atomiche (opcodes + dati relativi) che la rendono *digeribile* al nostro pezzo di silicio che comprende solo 1 e 0.

Facciamo attenzione a non mischiare due concetti: gli *opcodes* rappresentano le istruzioni in sé, esclusi i dati su sui operano, mentre quando si parla di *bytecode* si intende invece l'insieme degli opcodes supportati. Sebbene il bytecode della DVM non sia compatibile con quello Java, i suoi opcodes sono disegnati per supportare solo il linguaggio Java. Ci sono stati tentativi di compilare altri linguaggi in modo da produrre un bytecode compatibile con la DVM, ma la cosa è ostica proprio perché gli opcodes sono pensati proprio per Java. In figura 1, tratta dall'ottimo lavoro di Gabor Paller, abbiamo un estratto degli opcodes della DVM. Per la lista completa si veda il box link utili. Notiamo che si tratta di codici a 2 Bytes (4 caratteri Hex), dove Vx rappresenta il registro X della DVM. Operazioni che usano valori di tipo *long* o *double* usano due registri consecutivi (es. V0 e V1). Tutti gli esempi riportati di riferiscono ad una architettura di processore *big-endian*, ovvero una istruzione rappresentata dalla sequenza 0F00 0A00 sarà codificata in memoria come 0F, 00, 0A, 00. Per comprendere meglio la relazione tra gli opcodes Java e DEX, dobbiamo seguire l'intero processo di conversione. Si parte dal sorgente Java. L'ambiente di sviluppo Android, tramite il compilatore Java, produrrà quindi un file .class. Qui entra in gioco il programma DX (DEXER), parte dello SDK di Android, che converte il file .class nel formato DEX. Abbiamo così appreso che la differenziazione avviene nell'ultimo passo.

COSA È POSSIBILE OGGI?

Alt! Poniamoci delle domande. Innanzitutto, cosa vuol dire disassemblare? E poi, quali obiettivi ci proponiamo di raggiungere? La risposta alla prima domanda sembra facile, ma in realtà è la più complessa proprio in ragione dei passi visti in precedenza. Quindi partiamo dalla seconda, sfatando subito una aspettativa. Ad oggi non esiste alcun sistema affidabile per riportare un file DEX al file .class da cui si è partiti. E allora? E allora vuol dire che non riusciremo ad arrivare al sorgente Java di partenza bello e pronto (da un .class si può risalire al .java che lo ha generato).
Ma aspettate a chiudere l'articolo: dobbiamo rispondere alla prima domanda. Disassemblare significa in essenza permetterci di comprendere il flusso di un programma traducendo la sua sequenza di 1 e 0 in istruzioni più facilmente comprensibili dall'uomo. La traduzione può avvenire a vari livelli, e sarebbe auspicabile poter sostituire quella sequenza da mal di testa in qualcosa il più comprensibile possibile.
In linea di principio, anche un editor Esadecimale è un primo livello di disassemblatore, ma possiamo comunque dire che il primo passo "efficace" è quello che porta a tradurre gli opcodes esadecimali nelle rispettive istruzioni. Il risultato sembrerà quello di un codice Assembler, ancora molto vicino al modo di pensare dello hardware.
E questo passo si può fare. Anche se non così "human-friendly" come un sorgente in Java, ci permetterà comunque di seguire la logica del programma. E i programmi migliori, come vedremo, fanno un buon lavoro.

DEX VS ODEX

Prima di procedere c'è un aspetto poco noto da considerare. Alla prima esecuzione di un programma, la DVM fa alcune operazioni sul file DEX. Intanto una verifica di correttezza del bytecode (ci interessa relativamente), ma sopratutto ne effettua l'ottimizzazione. Il processo DEXOPT carica il DEX, lo analizza e lo ottimizza per la DVM. Quindi scrive il risultato (detto ODEX - DEX Ottimizzato) nella cache della DVM (/data/dalvik-cache). Notate che questa ottimizzazione rende l'ODEX non portabile tra DVM diverse. Per comprendere il problema della portabilità basta osservare cosa fa DEXOPT. Intanto rimpiazza certe istruzioni con altre più efficaci per la particolare architettura su cui la DVM gira. Quindi applica il corretto schema little-endian/big-endian e allinea le strutture dati di conseguenza. In particolare tutte le strutture dati sono allineate ai 4 o 8 Bytes.

Opcode (hex)	Opcode name	Explanation	Example
00	nop	No operation	0000 - nop
01	move vx,vy	Moves the content of vy into vx. Both registers must be in the first 256 register range.	0110 - move v0, v1 Moves v1 into v0.
02	move/from16 vx,vy	Moves the content of vy into vx. vy may be in the 64k register range while vx is one of the first 256 registers.	0200 1900 - move/from16 v0, v25 Moves v25 into v0.
03	move/16		
04	move-wide		
05	move-wide/from16 vx,vy	Moves a long/double value from vy to vx. vy may be in the 64k register range while vx is one of the first 256 registers.	0516 0000 - move-wide/from16 v22, v0 Moves v0 into v22.
06	move-wide/16		
07	move-object vx,vy	Moves the object reference from vy to vx.	0781 - move-object v1, v8 Moves the object reference in v8 to v1.
08	move-object/from16 vx,vy	Moves the object reference from vy to vx, vy can address 64k registers and vx can address 256 registers.	0801 1500 - move-object/from16 v1, v21 Move the object reference in v21 to v1.
09	move-object/16		
0A	move-result vx	Move the result value of the previous method invocation into vx.	0A00 - move-result v0 Move the return value of a previous method invocation into v0.

Estratto della lista di opcodes della Dalvik Virtual Machine (tratta dall'ottimo lavoro di Gabor Paller)

LA JASMIN SINTAX

Ci serve un ulteriore pezzo del nostro complesso puzzle.
Jasmin nasce come un Assembler per Java, fornito a supporto di un libro sulla JVM visto che all'epoca SUN non forniva un Assembler Java. Rapidamente è diventato uno standard. Di fatto permette di convertire una descrizione ASCII delle classi Java nel corrispondente codice binario.
Leggere la sua sintassi, ad oggi arrivata alla versione 2.0, richiede impegno perché assomiglia ad un misto tra Assembler e Java. Ad esempio le direttive tipiche dell'Assembler sono arricchite da parole chiave tipiche di Java (tipo ".class", ".interface", ".implements", ".method", etc.)
Per i nostri scopi serve sapere che questa sintassi è utilizzata dai principali disassemblatori Java. In altri termini, molti di essi producono un sorgente che rispetta questa sintassi. Quindi è utile studiarla bene.

TOOL DISPONIBILI

Fatte queste necessarie premesse, possiamo passare agli strumenti che la rete ci mette a disposizione.
Partiamo da quello fornito dai ragazzi di Google. Anche se non pubblicizzato, Android arriva già completo di un disassemblatore. Si tratta di **dexdump**. Uno strumento spartano, che si lancia da linea di comando. Esempio, per disassemblare il nostro file classes.dex, dovremo digitare:

```
adb shell
dexdump -d classes .dex
```

Per darvi una idea del suo output, osserviamo una semplice istruzione di switch Java che assegna ad una variabile i valori 15, o 2, o 5, o 6:

```
000418: 2b02 0c00 0000                  |0000:
packed-switch v2, 0000000c // +0000000c
00041e: 12f0                            |0003:
const/4 v0, #int -1 // #ff
000420: 0f00                            |0004:
return v0
000422: 1220                            |0005:
const/4 v0, #int 2 // #2
000424: 28fe                            |0006:
goto 0004 // -0002
000426: 1250                            |0007:
const/4 v0, #int 5 // #5
000428: 28fc                            |0008:
goto 0004 // -0004
00042a: 1260                            |0009:
const/4 v0, #int 6 // #6
00042c: 28fa                            |000a:
goto 0004 // -0006
00042e: 0000                            |000b:
nop // spacer
000430: 0001 0300 faff ffff 0500 ...
|000c: packed-switch-data (10 units)
```

Non ci ricorda il vecchio disassemblatore presente con il MSDOS? Insomma: dexdump fa un lavoro un po' migliore della semplice traduzione degli opcodes, ma seguire il flusso di un programma complesso in questo modo non è facile.
Per questo motivo sono nati disassemblatori più evoluti. Nel nostro caso in particolare dobbiamo fare riferimento a **dedexer**, la cui ultima versione è, attualmente, la **ddx1.14**.

Dedexer è un'applicazione Java che usa la JVM standard. Richiede Java 1.6, ma potrebbe essere ricompilato con Java 1.5 per chi avesse una simile limitazione. Il suo formato di output è basato sulla sintassi Jasmin. Per lanciarlo si usa tipicamente:

```
java -jar ddx.jar -d <directory> <dex
file>
```

sostituendo <directory> con il nome completo della cartella in cui vogliamo che dedexer metta il suo output.
Con riferimento all'istruzione switch dell'esempio precedente, l'output di dedexer risulta molto più intuitivo:

```
.method public calc1(I)I
   packed-switch v2,0
      ps418_422  ; case 0
      ps418_426  ; case 1
      ps418_42a  ; case 2
      default: ps418_default
ps418_default:
   const/4  v0,15
l420:
   return   v0
ps418_422:
   const/4  v0,2
   goto l420
ps418_426:
   const/4  v0,5
   goto l420
ps418_42a:
   const/4  v0,6
   goto l420
   nop
.end method
```

Dedexer offre altri vantaggi pratici. Intanto crea sia un file separato per ogni classe Java, sia una struttura di directory che rappresenta la struttura del pacchetto, rendendo la successiva analisi molto più agevole.
C'è un punto a cui fare attenzione. L'applicazione mantiene internamente una lista degli opcodes Dalvik che non è necessariamente l'intero bytecode DVM. Sebbene con le ultime versioni la lista sia realmente di fatto esaustiva, l'autore chiede a chi trovi opcodes non noti di segnalarglieli. In altri termini, è bene tenere dedexer aggiornato. Sul sito si possono leggere informazioni sulle aree in cui deve ancora migliorare. In particolare vi segnalo che non gestisce (ancora) informazioni di debug e annotazioni, il che è un vero peccato. Al di là di ciò, è buono e utile, e lo sviluppatore è pronto ad aiutare.

Nella rete ci sono anche altri strumenti che possono far parte del nostro arsenale. Ad esempio l'accoppiata **smali** e **baksmali** (attualmente in versione 1.2.6). Si tratta di un assemblatore DEX e relativo disassemblatore. La sintassi è molto vicina alla Jasmin, e supportano tutte le funzionalità del formato DEX, incluse informazioni di debug e annotazioni. Sempre per i curiosi, smail e baksmali non sono i nomi di due divinità del Valhalla, ma semplicemente la traduzione Islandese delle

parole assemblatore e disassemblatore. Per vederlo in azione possiamo provare a disassemblare il classico esempio della programmazione: un'applicazione che stampi "Hello World!". Entrambi sono distribuiti con uno script omonimo (ma senza l'estensione jar) che fa la launcher e ne semplifica l'uso. Senza dilungarsi su questo wrapper, ben commentato, l'output disassemblato apparirà simile a questo:

```
.class public LHelloWorld;
.super Ljava/lang/Object;
.method public static main([Ljava/
lang/String;)V
   .registers 2
   sget-object v0, Ljava/lang/System;-
>out:Ljava/io/PrintStream;
   const-string v1, "Hello World!"
     invoke-virtual {v0, v1}, Ljava/
io/PrintStream;->println(Ljava/lang/
String;)V
   return-void
.end method
```

Anche se non è il sorgente Java originario, gli è comunque molto più vicino ed è comprensibile.
Una piccola annotazione: il lexer/parser utilizzato da smali è l'ottimo, potente e personalizzabile ANTLR V3.

CI FERMIAMO QUI?

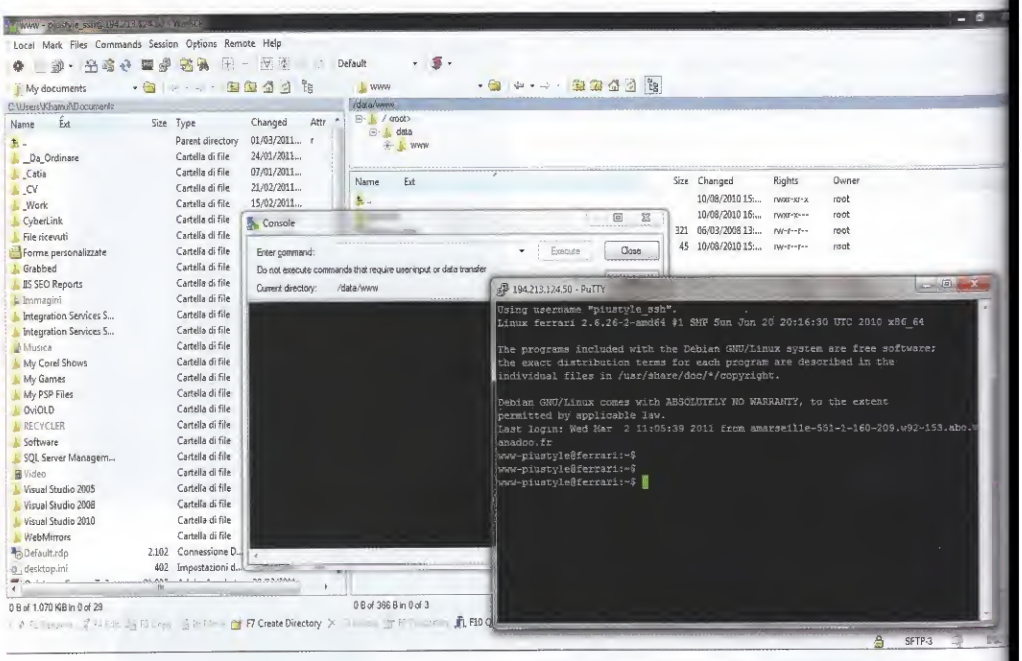
Per quello che offre attualmente il mercato ci dovremmo fermare qui. Ma ho lasciato per ultima una piccola sorpresa.
C'è infatti un ultimo programma su cui soffermarci: **dex2jar**.
La versione corrente è **dex2jar-0.0.7.8**. Anche esso, come bali/baksmali, è sulle pagine di progetti ospitati da Google-code. Dichiara di riuscire a convertire il formato DEX in formato .class Java. Cosa? Abbiamo sentito bene? E finora avevi detto che non si poteva! Calma... È un programma nuovo (nato nel luglio del 2010) e ancora non c'è quasi nulla della documentazione di supporto. Tuttavia l'esempio riportato sul sito sembrerebbe indicare che riesca nel suo intento (con il supporto di ulteriori utility, come JD). Chi lo usa dice però che per la maggior parte delle applicazioni va in crash e che riesce nel suo compito solo nei casi più semplici. Per questo motivo è ancora un po' presto per dire se questo sarà lo strumento che chiude il cerchio, ma vale la pena tenerlo d'occhio.

Link utili
I programmi referenziati, con gli esempi e la documentazione si trovano ai seguenti URL:
http://dedexer.sourceforge.net/
http://jasmin.sourceforge.net/
http://code.google.com/p/smali/
http://code.google.com/p/dex2jar/

Altri siti utili:
http://en.wikipedia.org/wiki/Dalvik_%28software%29
http://developer.android.com/reference/dalvik/bytecode/Opcodes.html
http://pallergabor.uw.hu/androidblog/dalvik_opcodes.html
http://jasmin.sourceforge.net/

Molti ormai sono i cellulari di nuova generazione che si avvalgono del sistema operativo Android.

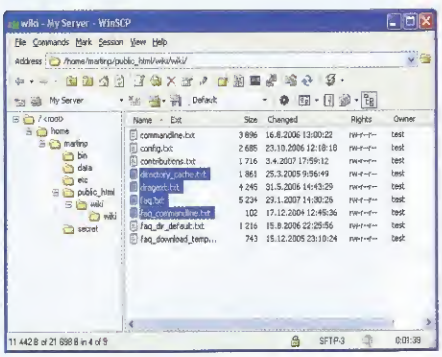
CONNETTERSI SSH



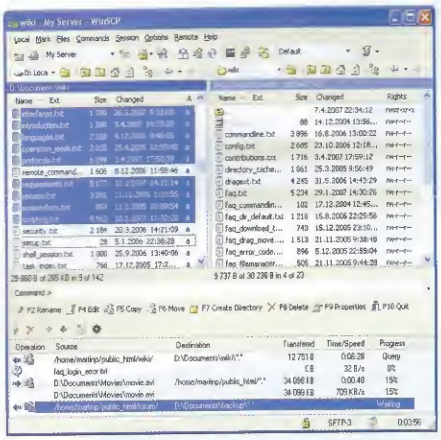
TUTTI CONOSCONO E USANO PUTTY MA WINSCP È UN CLIENT SSH ALTRETTANTO VALIDO E ANCHE PIÙ SEMPLICE DA USARE.

di M45t3R EWS
redazione@hackerjournal.it

Telnet è un protocollo di rete tra i più antichi dell'era IT ed è utilizzato essenzialmente per fornire a utenti remoti la possibilità di interagire con i sistemi tramite una interfaccia testuale. Malgrado sia usato da sempre, il suo livello di sicurezza lo rende una scelta tra le peggiori proprio per fornire il servizio per cui è nato. Innanzitutto Telnet non cifra alcun dato, password incluse, permettendo facilmente la cattura del traffico scambiato tra client e server. In più, Telnet non dispone di alcuno schema di autenticazione tra client e server, cosa che rende le applicazioni che si basano su questo protocollo estremamente vulnerabili. Per una comunicazione sicura è stato quindi necessario creare sistemi più avanzati, capaci di cifrare le comunicazioni, di dare sicurezza nella trasmissione dei dati e sopperire alle mancanze di Telnet.



L'uso dell'interfaccia simil Explorer di WinSCP non spaventa nessuno. Almeno fino a quando non si dà un'occhiata alla quantità di icone.



Nella modalità ereditata da Norton Commander, l'interfaccia di WinSCP appare complessa alla maggior parte degli utenti ma esprime tutte le potenzialità del programma.

Questo protocollo è il Secure Shell Connection, meglio noto come SSH. Questo protocollo crea un tunnel cifrato tra client e server che permette il trasporto di pacchetti TCP in modo sicuro, proteggendom la comunicazione da qualsiasi intercettazione e ottenendo come effetto collaterale di sbloccare qualsiasi limitazione al routing dei pacchetti in transito.

Grazie all'SSH è possibile, quindi, utilizzare una connessione non sicura, come qualsiasi connessione Internet standard, per il transito di informazioni sensibili. Dai principi usati per creare l'SSH sono stati poi derivati altri protocolli tra cui il più famoso è il TFTP che viene usato in sostituzione dell'FTP, il quale soffre di problemi simili a Telnet.

INDISPENSABILE

SSH e TFTP, quindi, sono accumunati da caratteristiche simili che li rendono i due protocolli più utilizzati per la gestione di server e computer da remoto. Entrambi usano connessioni sicure e cifrate, con autenticazioni basate su chiavi pubbliche per i server, che li identificano univocamente.

Ovvio, quindi, che uno strumento in grado di usarli entrambi, contemporaneamente, per la gestione di server remoti sia indispensabile nella valigia degli strumenti di qualsiasi sistemista. Per Windows, questo strumento si chiama WinSCP. È un client grafico open source che, ovviamente, permette lo scambio di dati in modo protetto ma che spinge l'utilizzo di SFTP e SSH ai loro massimi limiti.

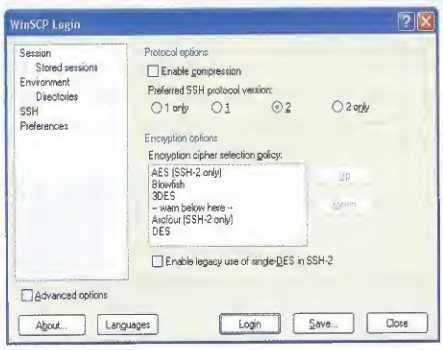
Disponibile in diverse lingue, tra cui l'italiano, è perfettamente integrato con Windows e supporta il Drag&Drop. Da un punto di vista delle funzioni a livello di applicazione, WinSCP è uno strumento indispensabile ai sistemisti: permette la creazione di script batch da eseguire anche a linea di comando, può mantenere sincronizzate directory locale e remote, ha un editor di testi integrato e può operare anche in modo standalone, senza necessità di installazione sul client. Specializzato nella gestione dei file, può interagire con Putty, che fa parte del suo pacchetto di installazione, e supporta pienamente l'uso di autenticazioni basate su chiave pubblica.

EXPLORER O NORTON COMMANDER?

Le operazioni supportate da WinSCP sono tutte quelle che ci si aspetterebbe da un programma di gestione di questo livello: upload e download di file, rinomina di file e directory, creazione di nuove directory, modifica delle proprietà e creazione di collegamenti. Risulta, quindi, un client molto simile a quelli FTP diffusi presso qualsiasi utente di medio livello, con la differenza di essere dedicato alla connettività protetta e, quindi, agli utenti più smaliziati e ai professionisti.
A causa della sua utenza fatta di esperti, in fase di installazione WinSCP permette di scegliere tra due modalità di utilizzo che, pur avendo le stesse funzioni di base, possono accontentare un'ampia gamma di utenti. La modalità standard è quella Explorer-like, che replica le funzioni di Windows Explorer e risulta più familiare alla maggior parte degli utenti medi. La modalità Norton Commander, invece, presenta una doppia finestra di contenuti come quella dei client FTP di alto profilo, come il ben più famoso FileZilla. Tra le altre cose, questa modalità permette di gestire con WinSCP anche i file locali.

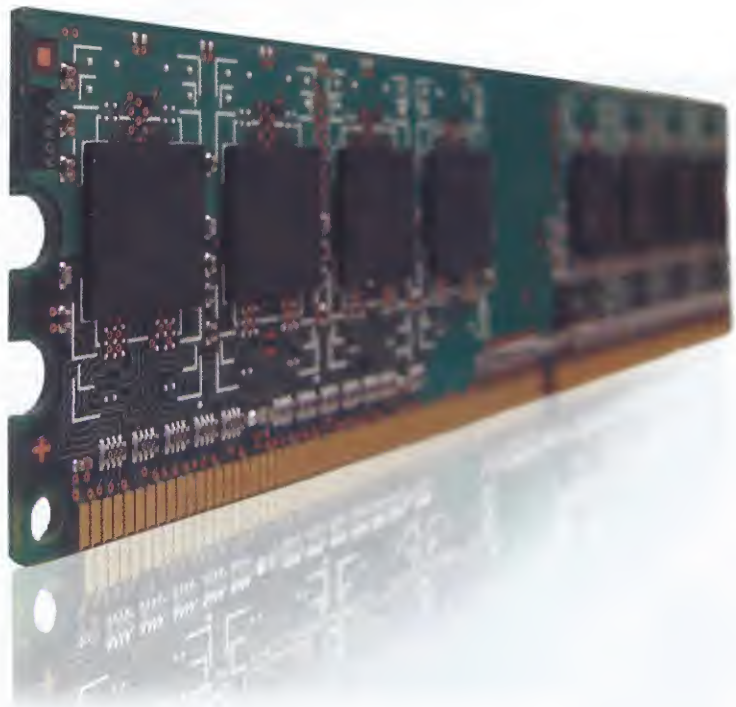
CONNETTI L'IPHONE

Come sistema di collegamento protetto, WinSCP non è detto che debba essere usato solo tra client e server. Un collegamento molto utilizzato è quello tra WinSCP e iPhone, iPad oppure iTouch. Il requisito è quello di aver installato OpenSSH su questi dispositivi e, quindi, di avere fatto ricorso al jailbreak. OpenSSH può poi essere installato come qualsiasi altra applicazione, tramite Icy, Cydia oppure Installer.app.
La connessione al dispositivo Apple tramite Wi-Fi è possibile inserendo l'IP del dispositivo sulla rete, come si farebbe con qualsiasi altro server. Occorre poi inserire *root* come nome utente e *alpine* come password. In alcune versioni del firmware del dispositivo la password è *dottie*. Dopo aver compilato la scheda, un clic su Login ci permetterà una connessione SSH al nostro dispositivo. Se la connessione non funziona al primo colpo, è consigliabile aumentare il tempo di attesa di risposta del server: alcuni dispositivi sono molto lenti.
I motivi per cui fare questo genere di collegamento sono facilmente intuibili: una connessione diretta tra computer e cellulare, per esempio, permette di trasferire suonerie e immagini in entrambi i sensi e senza alcun limite. Una possibilità di risparmio e personalizzazione impensabile a chi è legato ai numerosi blocchi imposti da Apple.



Sono molti i parametri di configurazione delle connessioni SSH: diverse varianti di protocollo, di attivare o meno la compressione e via dicendo.

IL RAMDISK CON WINDOWS 7



CHI L'HA DETTO CHE I RAM DISK NON SERVONO? CON TUTTA LA RAM CHE C'È DISPONIBILE...

di N4Break
redazione@hackerjournal.it

Diversi anni fa, i RAM disk erano l'ingrediente indispensabile di qualsiasi computer che avesse bisogno di prestazioni elevate: gli hard disk erano troppo lenti per essere utili e avere un disco virtuale in memoria permetteva di raggiungere performance impensabili con i dischi reali.

Lo scotto da pagare era monetario, visti i prezzi elevatissimi della RAM. Così, col passare del tempo e l'aumento delle prestazioni dei dischi reali, i RAM Disk sono andati svanendo e oggi sembrano essere solo un ricordo di chi ha più di 30 anni. In realtà sono ancora usati in alcuni contesti particolari ad altissime prestazioni, generalmente come dischi dedicati alla cache, per server che devono elaborare dati ad alta velocità: se un'applicazione non permette il caching dei dati in RAM ma solo in file su disco, questi file possono essere inseriti in un RAM disk.

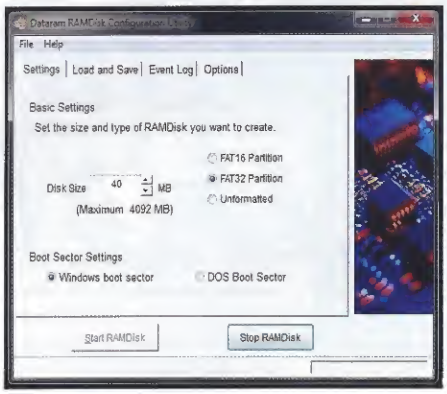
UN CONCETTO ATTUALE

Con tutta la quantità di memoria RAM disponibile oggi sui nostri sistemi, grazie al calo generalizzato dei prezzi di questa risorsa essenziale, anche i sistemi desktop possono trarre vantaggi dall'uso di questo tipo di dischi. Il concetto è semplice: se un desktop comprato d'occasione al supermercato dispone spesso di oltre 2 Gb di memoria RAM, perché non dedicarne qualche Mb (ma anche di più) a un disco?

Già con Windows XP c'erano smanettoni che riuscivano a convincere Windows, tramite DLL che fanno parte del processo di installazione di Windows e file .inf costruiti ad hoc, ad utilizzare una parte della memoria per ospitare i files.

Windows vedeva queste aree di memoria come nuove unità, del tutto virtuali ma indistinguibili da quelle fisiche, evitando che altri programmi le usassero per i loro scopi. A tutti gli effetti il thread del driver del RAM disk risultava grande qualche Kb più dell'area di memoria RAM dedicata al disco virtuale.

Quella che era solo una pratica di nicchia, però, è oggi un



La schermata principale di configurazione del programma è semplice da usare: con pochi clic possiamo decidere quanto grande vogliamo il disco e i suoi dati essenziali.

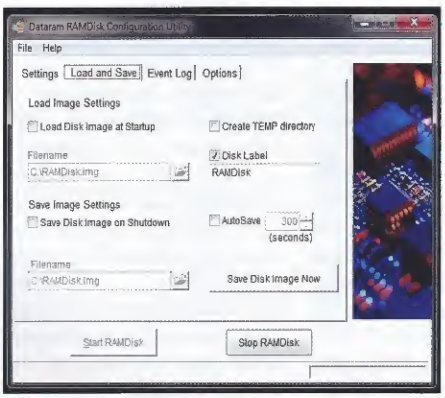
trend ufficializzato dall'uscita sul mercato di diversi tool che permettono di creare RAM disk grandi da pochi Mb a svariati Gb. Uno dei freeware più adatti a un computer desktop è Dataram RAMDisk, inserito anche nel nostro CD.
Per prima cosa è un programma totalmente gratuito se creiamo dischi di dimensione inferiore ai 4 Gb.
Considerando che stiamo trattando la memoria RAM, che costa poco ma non è gratis, si tratta di un provvedimento preso per assicurarsi che non venga usato nei server industriali senza pagamento di una licenza, per altro piuttosto economica. Quasi certamente, questa limitazione non sarà un problema, anche se potrebbe essere interessante disporre di così tanto spazio su un disco super veloce: i RAM disk possono essere usati come dischi a tutti gli effetti, spostandoci sopra ogni cache di sistema e ogni file temporaneo, ottenendo velocità di accesso e lettura impensabili con qualsiasi hard disk esistente.
Altro motivo per consigliarlo è che, diversamente da quanto accadeva con le soluzioni artigianali, le impostazioni di base di Dataram RAMDisk sono molto semplici: tramite un pannello di controllo possiamo indicare le dimensioni del disco, il tipo di partizionamento che vogliamo usare e il tipo di settore di boot. La stessa semplicità c'è anche per attivarlo e disattivarlo: basta un clic su uno dei bottoni disponibili per questo scopo.

DISASTRO!

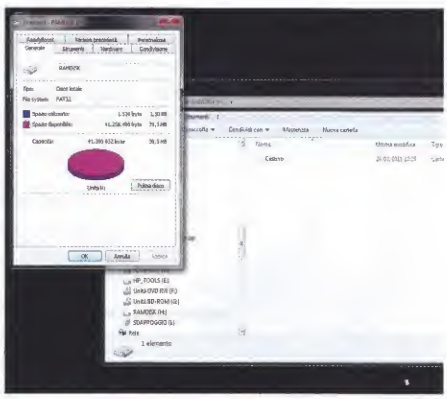
Di certo occorre fare attenzione alla scrittura su RAM disk dei file che vogliamo conservare: la memoria RAM si spegne con il computer e un reboot, volontario o meno, può essere fatale e farci perdere ore di lavoro oppure dati indispensabili.
Per questo motivo dobbiamo assolutamente evitare di mettere in un RAM disk qualsiasi file importante di cui non abbiamo una copia su un disco tradizionale. D'altra parte, tutti i file che infestano abitualmente le nostre directory TMP saranno i benvenuti: al reboot successivo della macchina, spariranno.

Il problema della persistenza dopo il reboot è nato con il concetto di RAM disk e, diversi anni fa, le soluzioni trovate erano le più disparate: da file batch che copiavano i file necessari nel RAM disk all'avvio a soluzioni sofisticate di riconfigurazione automatica di alcune applicazioni, che usavano come primo disco un RAM disk in failover su un disco reale. Soluzioni che oggi possiamo dimenticarci: Dataram RAMDisk può gestire queste funzioni direttamente tramite il suo driver, caricando automaticamente un disco immagine al boot. Per limitare al massimo i problemi causati da interruzioni elettriche possiamo impostare un tempo limite per il salvataggio periodico dell'immagine del disco. Usando una periferica veloce come la RAM, pilotata da un driver dedicato, abbiamo anche possibilità di controllo difficilmente replicabili con un disco tradizionale: Dataram RAMDisk può inserire nel nostro log di sistema le sue annotazioni, permettendoci un controllo totale dell'attività svolta tramite i normali strumenti di Windows.

Complessivamente il programma offre prestazioni decisamente buone, anche considerando la sua gratuità e l'impossibilità di creare dischi di dimensione superiore ai 4 Gb con la versione freeware non è certamente una limitazione da considerare su un computer desktop. Durante la sua installazione, comunque, facciamo attenzione a non dedicare troppa RAM al disco: se un solo Gb su un sistema che dispone di 4 Gb è tanto ma non mette in crisi Windows, impiegare come disco 250 Mb su un sistema che dispone di un Gb soltanto è dannoso.



Sulla schermata Load and Save possiamo impostare i parametri avanzati: un'immagine disco da caricare al boot, un salvataggio automatico a intervalli predeterminati e altro.



Windows non fa alcuna differenza di utilizzo tra un disco reale e un RAM Disk: possiamo anche deframmentarlo o avviare lo scandisk. Ovviamente non funzionerà come ReadyBoost.

HACKING
NEL CD

MI PRENDO IL TUO WI-FI

```
[00:00:00] Tested 2955 keys (got 24571 I

KB    depth   byte(vote)
 0    0/  1   4D(76025700) A9(67942200) D9(66881400) 5A(60
 1    1/  2   C7(68113050) F4(66014400) DC(64872000) 1F(64
 2    0/  1   6F(71114400) A0(67014000) BD(65351400) 96(64
 3    0/  1   34(72705600) FA(68541450) E4(66932400) CA(60
 4    0/  1   1B(60613500) 60(47736000) 77(47379000) 84(47
 5    0/  1   FF(60282000) F2(48960000) 5C(46920000) 98(46
 6    0/  9   90(48144000) F4(47672250) 00(46856250) DB(46
 7    0/  1   6A(71706000) A7(50184000) CA(48501000) 69(46
 8    0/  1   22(58089000) 86(46920000) 51(46499250) 69(45
 9    0/  1   13(57936000) 9E(52555500) 91(49368000) 29(47
10    1/  8   CE(49776000) 83(49368000) A3(49368000) D8(49
11   19/ 21   2B(41960250) E6(41718000) 77(41616000) A2(41
12    0/  1   D3(169932000) 40(169320000) E9(166668000) 7

        KEY FOUND! [ 4D:C7:6F:34:1B:FF:90:6A:22:13:CE:1
    Decrypted correctly: 100%
```

CIFRATURA INSICURA? ENTRO NELLA TUA WIRELESS IN 10 MINUTI. FORSE MENO.

di Little Rose
redazione@hackerjournal.it

Ormai sembra che chiunque abbia una connessione a Internet ce l'abbia Wi-Fi, anche se non sa esattamente cos'è. Basta girare per qualsiasi strada con un portatile acceso per ritrovarsi con liste lunghe km delle connessioni più disparate. La maggior parte di questi utenti, però, usa la propria wireless come un bambino gioca con le bombe a mano: non ha idea di come funziona e si diverte finché qualcosa non va storto. Lo storto, in questo caso, può non essere tanto grave perché potrebbe essere uno sconosciuto comodamente seduto in un bar, nei pressi dell'access point di questi malcapitati.

Non serve nemmeno una gran ricerca per addentrarsi in questo mondo: la suite AirCrack-NG, disponibile su molteplici piattaforme e inserita nel nostro CD in versione per Windows, mette a disposizione di chiunque gli strumenti necessari. Manca solo un portatile con una wireless dal chipset compatibile (vedere l'elenco al sito http://www.aircrack-ng.org/doku.php?id=compatibility_drivers).

IL PRIMO PASSO

Dopo aver confermato che il nostro chipset è compatibile, stoppiamo tutte le interfacce di rete del pc e avviamo solo la wireless in modalità monitor. Questo è necessario perché la nostra rete Wi-Fi, di solito, dà ascolto solo ai pacchetti che gli vengono indirizzati. In modalità monitor, invece, verrà ascoltato qualsiasi pacchetto riesca a catturare. C'è anche un'altra necessità: la nostra scheda non deve mettersi a comunicare con gli access point ma deve restare invisibile, silente, fino a quando non faremo una injection di pacchetti "speciali" nelle comunicazioni tra gli AP e i loro client legittimi----------.

Per prima cosa usiamo il comando airmong-ng sulle nostre interfacce di rete fisica per spegnerle. Per esempio: airmon-ng stop ath0 blocca l'interfaccia ath0. Il comando replicherà dandoci lo status dell'interfaccia prima e dopo la cura, segnalando la distruzione VAP. Usiamo il comando iwconfig per assicurarci che nessuna interfaccia ath sia funzionante. Questo perché le utility incluse in AirCrack-NG fanno uso di propri drivers che insistono direttamente sul chipset e la presenza di interfacce ath che incapsulano le interfacce wifi rende impossibile il loro utilizzo esclusivo. Se usiamo anche altri drivers che si comportano in modo simile, disattiviamoli allo stesso modo.

Ora avviamo il chipset wireless in modalità monitor sul canale usato dall'Access Point da attaccare usando il comando airmon-ng start wifi0 9, dove wifi0 è l'interfaccia e 9, in questo caso, il numero del canale. Questo passo è indispensabile per catturare correttamente i pacchetti, usati per la decodifica della password. Una volta dato il comando, il sistema risponderà segnalando l'attivazione del monitor mode sull'interfaccia. Non fidiamoci e controlliamo con iwconfig l'attivazione, assicurandoci anche che venga esposto, nella risposta, il MAC address della scheda. Sarà indice che stiamo usando i driver corretti di AirCrack-NG.

PRIMO CADEAU

Adesso proviamo a mandare al mondo il nostro primo pacchetto, ovviamente palesemente falso. Basta un comando tipo: aireplay-ng -9 -e testme -a 00:13:5B:3C:42:73 ath0. Il comando vero e proprio è AirePlay-NG, seguito da -9 che avvia un injection test, da -e con il nome della rete, da -a con il MAC address dell'AP da colpire e il nome dell'interfaccia che usiamo. Se tutto va a buon fine dovremmo vederci rispondere con delle statistiche riguardanti il nostro ping e una percentuale di successo dell'operazione. Se questa sarà bassa, siamo troppo lontani dall'AP e conviene avvicinarci un po'. Se sarà zero, invece, brutte notizie: stiamo usando driver wireless non compatibili o malfunzionanti (non perdiamo subito le speranze: controlliamo gli update sul sito del produttore).

ADESSO TI PRENDO!

Ora è tutto pronto e predisposto e sarebbe bello poter dire che ora inizia la parte divertente. Ma non è così e questa è, in realtà, la parte più noiosa: catturare gli IV generati a scopo di analisi. Useremo il comando Airo-Dump-NG seguito dalla specifica del canale usato, dal MAC dell'Access Point vittima, da un nome del file dove vogliamo salvare il traffico intercettato e dal nome dell'interfaccia che usiamo. Il risultato finale è un comando come questo: airodump-ng -c 9 --bssid 00:13:5B:3C:42:73 -w output ath0. Lasciamo girare questo programma per un po', fino a ricevere una schermata riassuntiva delle informazioni raccolte.

Adesso torniamo alla parte divertente: perché il tentativo funzioni, dobbiamo assicurarci che il MAC address della nostra scheda Wireless sia correttamente associata all'Access Point vittima. Diversamente, l'access point vittima invierà un DeAutentication packet, ignorandoci. Tentiamo quindi l'autenticazione usando il comando AirePlay-NG -1 0 -e testme -a 00:13:5B:3C:42:73 -h 00:0F:B5:88:AC:82 ath0. Tradotto in modo umano significa: tenta un'autenticazione fake (-1) facendo una riassociazione immediata (0 secondi), sul network testme (-e testme) con l'access point che ha MAC address 00:13:5B:3C:42:73 (-a 00:13:5B:3C:42:73) dalla card Wi-Fi che ha MAC address 00:0F:B5:88:AC:82 (-h 00:0F:B5:88:AC:82) sull'interfaccia ath0. Il comando AirePlay-NG può essere variato con un unico tentativo di connessione ma per più tempo, con qualche parametro in più: areplay-ng -1 5000 -o 1 -q 10 -e testme -a 00:13:5B:3C:42:73 -h 00:0F:B5:88:AC:82 ath0. In pratica usiamo un tempo di rinnovo dell'autenticazione di 5000 secondi, generando traffico di pacchetti keep-alive. Con la specifica del parametro -o 1, indichiamo al programma di inviare un pacchetto alla volta mentre il parametro -q 10 indica di inviare un keep-alive ogni 10 secondi. La scritta autentication successful indicherà che è ora di sorridere perché avremo fatto il grosso del lavoro. In caso di fallimento, nel log, potremo notare la ricezione del famigerato DeAuthentication packet, dopo il quale le nostre ulteriori richieste verranno ignorate, fino al cambio del nostro MAC address.

Ricordiamoci che abbiamo a che fare con un Access Point moderno e teorizziamo il peggior scenario possibile. Possiamo, quindi, avere a che fare con un AP che filtra i MAc address sulla base di una lista in suo possesso e sgancia tutti gli altri. Se fosse così, interrompiamo il lavoro e dedichiamoci a recuperare almeno un indirizzo di questa lista. per esserne certi, consultiamo il registro degli errori dell'interfaccia usata e guardare dalle parti dell'arrivo del DeAuthentication packet. Ora dovremo configurare il nostro chipset per la cattura dei pacchetti ARP. Questi sono una ghiotta preda per il nostro software di analisi: vengono normalmente rilanciati dall'AP e provocano la generazione di molti IV in poco tempo.

PRESO!

Lanciamo ancora AirePlay-NG con i parametri -3 -b 00:13:5B:3C:42:73 -h 00:0F:B5:88:AC:82 ath0 che avvierà il programma in ascolto dei pacchetti ARP. In un'altra sessione, avviamo immediatamente anche il programma AiroDump-NG per catturare il traffico che riusciamo a generare. Il numero di pacchetti scambiati dovrebbe crescere molto rapidamente, basta un'occhiata nella sessione di AiroDump-NG. In caso di perdita di associazione con l'Access Point, riceveremo un messaggio d'errore e dovremo ripeterla. Il numero di pacchetti necessari per la ricerca della password è variabile in base alle dimensioni della chiave. Chiavi a 128 bit richiedono fino a 1 milione e mezzo di pacchetti mentre ne bastano 250000 per chiavi a 32 bit. Ora, finalmente, tentiamo la decodifica della chiave della rete Wi-Fi. Lanciamo il comando AirCrack-NG -b 00:13:5B:3C:42:73 captured *.cap, con cui indichiamo a AirCrack-NG di trovare la password per l'Access Point che ha il MAC address indicato e il cui traffico catturato è nei file captured*.cap. Possiamo anche usare un metodo di decodifica diverso dallo standard speficando il parametro -K: aircrack-ng -K -b 00:13:5B:3C:42:73 captured *.cap. Questo secondo metodo rende necessario l'uso di meno pacchetti (85.000 per chiavi a 128 bit) ma non funziona su tutti i tipi di cattura.

Spesso non sarà necessaria l'analisi di tutti i pacchetti per arrivare a un risultato ma... Diamoci tempo e aspettiamo con pazienza. Se la cifratura è WEP, la suite AirCrack-NG ci servirà la chiave su un piatto d'argento. Se non è WEP, invece, possiamo consultare il sito di AirCrack-NG e i wiki contenuti, www.aircrack-ng.org, per i parametri necessari ad altri tipi di attacco. C'è un motivo importante per cui consigliamo vivamente a tutti di usare sulle Wi-Fi una cifratura WPA-PSK2!

Prepariamoci ad avere aperte diverse finestre di shell ma anche a ricevere tante soddisfazioni: AirCrack-NG è una suite d'oro!

Gli Access Point sono sicuri. Sono gli utenti che li configurano che, spesso, danno i maggiori problemi.